**Universidad de la República**
**Facultad de Ciencias**
**Centro de Matemática**

**Anillos**

Notas adaptadas por Mariana Haim para el curso "Anillos y Módulos" 2021.

## 0.1. Generalidades

**Definición 0.1.1** (Anillo)**.** Un anillo es una quíntupla $(A, +, \cdot, 0, 1)$ donde

(A1) $(A, +, 0)$ es un grupo abeliano,

(A2) $(A, \cdot, 1)$ es un monoide,

(A3) Propiedad distributiva: $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$, $\forall a, b, c \in A$.

Si además se cumple $a \cdot b = b \cdot a$ $\forall a, b \in A$ se dice que el anillo es *conmutativo*. Cuando las operaciones y los neutros se sobreentienden, decimos "el anillo $A$" en lugar de "el anillo $(A, +, \cdot, 0, 1)$". Las operaciones $+$ y $\cdot$ se llaman usualmente la *suma* y el *producto* de un anillo.

*Observación* 0.1.1. La definición anterior merece dos aclaraciones:

- Algunas definiciones de *anillo* que aparecen en la literatura no exigen la existencia de neutro para $\cdot$ y llaman *anillo con unidad* a una quíntupla como la de la definición 0.1.1.
- A menudo notaremos $ab$ en lugar de $a \cdot b$, para $a, b \in A$.

**Ejemplos 0.1.1** (Anillos)**.**

1. Los enteros con la suma y el producto usual $(\mathbb{Z}, +, \cdot, 0, 1)$.
2. Los reales con la suma y el producto usual $(\mathbb{R}, +, \cdot, 0, 1)$.
3. El anillo de las matrices cuadradas de tamaño $n \in \mathbb{N}$ con coeficientes en $\mathbb{R}$, con la suma y el producto usual de matrices $(M_n(\mathbb{R}), +, \cdot, 0, I_n)$. Es un anillo no conmutativo $\forall n \geqslant 2$.
4. El anillo trivial $A = \{0\}$ con $0 = 1$.
5. De manera similar al ejemplo anterior, si $A$ es un anillo y $n$ un natural, puede definirse una suma y un producto en el conjunto de las matrices cuadradas de tamaño $n$ con coeficientes en $A$ y se obtiene un anillo que se nota $M_n(A)$. Es no conmutativo $\forall n \geqslant 2$ si $A$ no es el anillo trivial.
6. El anillo de los polinomios en una variable con coeficientes en $\mathbb{R}$, con la suma y el producto usual de polinomios $(\mathbb{R}[x], +, \cdot, 0, 1)$. Es un anillo conmutativo.
7. El ejemplo anterior puede generalizarse a polinomios con coeficientes en un anillo $A$. Este anillo se nota $A[x]$.[1] Es claro que $A[x]$ es conmutativo si y sólo si $A$ lo es.
8. Si $A$ es un anillo y $S$ es un conjunto no vacío, el conjunto de las funciones de $S$ en $A$ se nota $A^S$ o también $\mathrm{Fun}(S, A)$, y es un anillo con las operaciones heredadas de $A$, es decir $(f + g)(s) = f(s) +_A g(s), (f \cdot g)(s) = f(s) \cdot_A g(s), \forall s \in S$. Si $A$ es un conmutativo, también lo es $A^S$.

[1] En la sección 0.3 daremos una construcción formal de $A[x]$.

**Proposición 0.1.1** (Propiedades elementales)**.** *Sea $(A, +, \cdot, 0, 1)$ un anillo. Entonces:*

1. *$0$ y $1$ son únicos.*
2. *Para todos $a, b \in A$: $(-a) \cdot b = -(ab) = a \cdot (-b)$, $(-a) \cdot (-b) = a \cdot b$.*
3. *Para $a \in A, n \in \mathbb{Z}$, notamos $na = \begin{cases} a + a \cdots + a \ \ (n\text{veces}) & \text{si } n \geqslant 0 \\ (-a) + (-a) + \cdots + (-a) \ (n\text{veces} & \text{si } n < 0 \end{cases}$.*
   *Se tiene, para $n \in \mathbb{Z}, a, b \in A$ las siguientes igualdades:*

$$(na) \cdot b = n(a \cdot b) = a \cdot (nb).$$

*Demostración.* A cargo del lector. □

**Definición 0.1.2.** Decimos que $a \in A$ es *invertible*, si existe $b \in A$ tal que $a \cdot b = b \cdot a = 1$.

*Observación* 0.1.2. Es fácil ver que para cada $a \in A$ existe un único $b \in A$ como en la definición. Decimos que es el *inverso* de $a$ y lo notamos $a^{-1}$.

**Proposición 0.1.2.** *Sea $(A, +, \cdot, 0, 1)$ un anillo no trivial. Si definimos $A^\times = U(A) := \{a \in A \mid a \text{ es invertible}\}$, la terna $(U(A), \cdot, 1)$ es un grupo.*

*Demostración.* Primero veamos que si $a, b \in A$ son invertibles, entonces $ab$ también lo es, y su inverso es $b^{-1}a^{-1}$. En efecto $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$. El producto es entonces una operación en $U(A)$, que además es asociativa.
Por otra parte 1 es invertible ($1 \cdot 1 = 1$ luego $1^{-1} = 1$), por lo que $U(A)$ tiene neutro.
Finalmente, todo elemento de $U(A)$ es invertible por definición. □

**Ejemplos 0.1.2** (Invertibles)**.**

- $U(M_n(\mathbb{R})) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$.
- $U(\mathbb{R}[x]) = \{p \in \mathbb{R}[x] \mid p \text{ constante } p \neq 0\}$.

**Definición 0.1.3** (Subanillo)**.** Sea $(A, +, \cdot, 0, 1)$ un anillo. Un subconjunto $B \subseteq A$ se dice *subanillo* si $B$ es un subgrupo de $(A, +, 0)$ y $B$ es un submonoide de $(A, \cdot, 1)$.

**Ejemplo 0.1.1.** $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ son dos a dos subanillos.

**Proposición 0.1.3.** *Sea $(A, +, \cdot, 0, 1)$ un anillo, $B \subset A$ un subconjunto. Son equivalentes:*

1. *$B$ es un subanillo de $A$,*
2. *$1 \in B$ y $a, b \in B \Rightarrow a - b \in B$ y $ab \in B$,*
3. *$(B, +_{|B\times B}, \cdot_{|B\times B}, 0, 1)$ es un anillo.*

*Demostración.* A cargo del lector. □

**Definición 0.1.4** (Morfismo de anillos)**.** Sean $A, B$ anillos y $f : A \to B$ una función. Decimos que $f$ es un *morfismo de anillos* si:

- $f(a + b) = f(a) + f(b) \quad \forall a, b \in A$,
- $f(ab) = f(a)f(b) \quad \forall a, b \in A$,
- $f(1_A) = 1_B$.

Un morfismo de anillos $f$ se dice *monomorfismo, epimorfismo* o *isomorfismo de anillos* si es respectivamente inyectivo, sobreyectivo o biyectivo.

Dos anillos $A$ y $B$ se dicen *isomorfos* (o *isomorfos via* $f$) si existe un isomorfismo de anillos $f : A \to B$.

Un *endomorfismo* de $A$ es un morfismo de anillos $A \to A$. Notaremos $\mathrm{End}(A)$ al conjunto de endomorfismos de $A$.

Un endomorfismo que es un isomorfismo se dice un *automorfismo*. Notaremos por $\mathrm{Aut}(A)$ al conjunto de automorfismos de $A$.

*Observación* 0.1.3.

1. Es claro que si $f : A \to B$ un morfismo de anillos en particular $f : (A, +_A, 0_A) \to (B, +_B, 0_B)$ es morfismo de grupos y $f : (A, \cdot_A, 1_A) \to (B, \cdot_B, 1_B)$ es morfismo de monoides. Entonces $f(0) = 0, f(-a) = -f(a) \ \ \forall a \in A$, por i $a \in A$ es invertible, entonces $f(a) \in B$ es invertible y $f(a)^{-1} = f(a^{-1})$. En otras palabras, $f_{|U(A)} : U(A) \to U(B)$ es un morfismo de grupos (con la estructura de grupo en los invertibles definida en la proposición 0.1.2).

2. Considerando a $f$ como morfismo de grupos bajo las estructuras aditivas de $A$ y $B$, se tiene que se pueden definir $Ker(f)$ e $Im(f)$ y además:

   - $\mathrm{Im}(f) \subseteq B$ es un subanillo.
   - $\mathrm{Ker}(f) \subseteq A$ es un subgrupo aditivo.

3. La composición de morfimos de anillos es un morfismo de anillos, la identidad es un morfismo de anillos, la inversa de un morfismo de anillos biyectivo es un morfismo de anillos. En otras palabras $\mathrm{Aut}(A)$ es un grupo con la composición.

4. Es necesario pedir que un homomorfismo de anillos $f : A \to B$ cumpla $f(1) = 1$. Si bien todo morfismo de grupos cumple automáticamente que $f(0) = 0$, esto no es cierto para los monoides, por lo tanto debemos pedirlo si queremos que $f$ respete la unidad. Por ejemplo, sea $f : \mathbb{R} \to M_2(\mathbb{R})$ definida por $f(a) = \left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Entonces $f$ respeta la suma y el producto, pero $f(1) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

## 0.2. Anillos especiales y ejemplos

Es claro que la igualdad $ab = 0$ en un anillo no implica $a = 0$ o $b = 0$ (basta mirar un anillo de matrices por ejemplo). Esta propiedad es interesante y muy útil en esta teoría, por lo que tiene relevancia la siguiente definición.

**Definición 0.2.1** (Divisor de cero)**.** Sea $A$ un anillo. Un elemento $a \in A, a \neq 0$ se dice *divisor de cero* si existe $b \in A, b \neq 0$, tal que $ab = 0$ o $ba = 0$.

**Ejemplos 0.2.1** (Divisores de cero)**.**

- La matriz $A = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ es un divisor de cero en $M_2(\mathbb{R})$ (se verifica por ejemplo $A \cdot A = 0$ y $A \neq 0$).

- Sea $A$ un anillo no trivial. En el anillo $A^S$, toda función no nula que admite una raíz es divisor de cero. En efecto, si $f : S \to A$ es no nula y tal que para cierto $s \in S$ se tiene $f(s) = 0$, entonces, tomando $g : S \to A$ tal que $g(t) = 0 \forall t \neq s$ y $g(s) \neq 0$, se tiene $(fg)(x) = 0, \forall x \in S$ y $g \neq 0$.

*Observación* 0.2.1. Los invertibles no son divisores de cero. En efecto, tomemos $a, b \in A$ tal que $ab = 0$. Si $a$ es invertible, entonces $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$. Análogamente se prueba que si $ba = 0$ entonces $b = 0$.

Algunos anillos tienen buenas propiedades que tienen que ver con sus invertibles y sus divisores de cero. Los presentamos en la siguiente definición.

**Definición 0.2.2.** Sea $A$ un anillo, $A \neq \{0\}$. Decimos que $A$ es un

- *dominio de integridad*, *dominio íntegro*, o simplemente *dominio* si es conmutativo y no tiene divisores de cero,
- *anillo con división* si todo elemento no nulo es invertible,
- *cuerpo* si es un anillo con división conmutativo.

*Observación* 0.2.2. De la observación 0.2.1 se deduce que todo cuerpo es un dominio.

**Ejemplos 0.2.2** (Anillos especiales)**.**

1. Todo cuerpo es un dominio.
2. Cualquier subanillo de un dominio es un dominio. En particular los subanillos de $\mathbb{R}$ son dominios, como por ejemplo $\mathbb{Z}, \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}, \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
3. El subanillo (conmutativo) $C[0,1] \subseteq \mathbb{R}^{[0,1]}$ de las funciones continuas en $[0,1]$ a valores reales no es un dominio.
4. Consideremos en $\mathbb{R}^4$ una base que notaremos $\{1, i, j, k\}$. Consideremos el conjunto $\mathbb{H} = \{a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\} = \mathbb{R}^4$ con la suma definida mediante:

   $$(a1 + bi + cj + dk) + (a'1 + b'i + c'j + d'k) = (a + a')1 + (b + b')i + (c + c')j + (d + d')k$$

   para todo $a, a', b, b', c, c', d, d' \in \mathbb{R}$, y el producto definido a partir de

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

   y extendiendo por linealidad. Se puede ver que esto define una estructura de anillo en $\mathbb{H}$. Este anillo recibe el nombre de *anillo de los cuaterniones* y es un ejemplo de anillo con división que no es un cuerpo. En efecto, todo elemento no nulo $a1 + bi + cj + dk$ tiene por inverso a $\frac{1}{a^2+b^2+c^2+d^2}(a1 - bi - cj - dk)$. Por otra parte, $\mathbb{H}$ no es conmutativo.
5. Para $n \geqslant 2$ y $A \neq \{0\}$, el anillo de matrices $M_n(A)$ no es un dominio.

**Definición 0.2.3** (Subanillo generado)**.** Si $S \subset A$ es un subconjunto de un anillo, el *subanillo generado* por $S$ es $\langle S \rangle := \bigcap \{B \mid B \text{ es subanillo de } A, B \supset S\}$.

## 0.3. Series formales y polinomios

### 0.3.1. Series formales con coeficientes en un anillo $A$

Dado un anillo consideramos el conjunto $A^{\mathbb{N}}$ de sucesiones con términos en $A$. Definimos en $A^{\mathbb{N}}$ las operaciones

$$(f + g)(n) = f(n) + g(n), \quad (f \star g)(n) = \sum_{k+l=n} f(k)g(l),$$

y las funciones $0, \delta_n : \mathbb{N} \to A$ dadas por $0(k) = 0, \forall k \in \mathbb{N}$ y $\delta_n(k) = \begin{cases} 1 & \text{si } n = k \\ 0 & \text{si no} \end{cases}$.

En este contexto, la siguiente observación es fácil de verificar.

*Observación* 0.3.1.

- $(A^{\mathbb{N}}, +, \star, 0, \delta_0)$ es un anillo. El producto se llama *producto de convolución*, *producto de Cauchy* o sencillamente *convolución*, y es conmutativo si y sólo si $A$ es un anillo conmutativo.
- Si definimos $x = \delta_1$ (que llamaremos la *indeterminada*), entonces $x^n = \delta_n, \forall n \in \mathbb{N}$.
- Para cada $n \in \mathbb{N}$, la aplicación $\varphi_n : A \to A^{\mathbb{N}}$ definida por $\varphi_n(a)(k) = \begin{cases} a & \text{si } n = k \\ 0 & \text{si no} \end{cases}$ es un monomorfismo de grupos que verifica $\varphi_n(ab) = \varphi_0(a)\varphi_n(b), \forall a, b \in A$ y $\varphi_n(1) = x^n$. En particular $\varphi_0$ es un monomorfismo de anillos.

A partir de la observación anterior, podemos escribir los elementos de $A^{\mathbb{N}}$ como:

$$(a_n)_n = \sum_{n=0}^{\infty} \varphi_n(a_n) = \sum_{n=0}^{\infty} \varphi_n(a_n \cdot 1) = \sum_{n=0}^{\infty} \varphi_0(a_n) \star x^n = \sum_{n=0}^{\infty} a_n x^n,$$

donde en la última igualdad, estamos haciendo un doble abuso de notación: identificamos el anillo $A$ con su copia en $A^{\mathbb{N}}$ y eliminamos la $\star$ del producto de convolución.

Por esta razón es que este anillo recibe el nombre de *anillo de las series formales (en una variable) con coeficientes en A*. Decimos que $a_n$ es el *coeficiente n-ésimo* de la serie $\sum_{n=0}^{\infty} a_n x^n$. El anillo se nota $A[[x]]$ y bajo la nueva notación, las operaciones se explicitan como sigue:

$$\left(\sum_{n=0}^{\infty} a_n x^n\right) + \left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} (a_n + b_n) x^n,$$

$$\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} \left(\sum_{k+\ell=n} a_k b_\ell\right) x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n.$$

A partir de ahora notaremos $fg$ para $f \star g$.

### 0.3.2. Polinomios con coeficientes en un anillo $A$

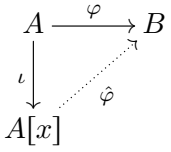
Dado $f \in A^{\mathbb{N}}$, definimos el *soporte* de $f$ como $\text{sop}(f) = \{n \in \mathbb{N} \mid f(n) \neq 0\}$. El subconjunto $\{f \in A[[x]] \mid \sharp\text{sop}(f) < \infty\}$ es un subanillo de $A$ que llamamos *anillo de polinomios con coeficientes en A* y notamos $A[x]$. Más específicamente, cada elemento de $A[x]$ se dice *polinomio con coeficientes en A*.

Es fácil ver que $A[x]$ es un anillo conmutativo si y sólo si lo es $A$. Más aún, $A[x]$ es el subanillo de $A[[x]]$ generado por $A \cup \{x\}$.

Observar que se tiene la cadena de inclusiones de anillos: $A \subset A[x] \subset A[[x]]$ (donde un elemento $a \in A$ se piensa en $A[x]$ como el polinomio con soporte $\{0\}$ y único coeficiente $a$).

**Teorema 0.3.1** (Propiedad universal del anillo de polinomios)**.** *Sea $\varphi : A \to B$ un morfismo de anillos. Para cada elemento $b \in B$ que conmuta con $Im(\varphi)$ existe un único morfismo de anillos $\hat{\varphi} : A[x] \to B$ y $\varphi(x) = b$ que extiende a $\varphi$.*

*En otras palabras, para cada $b \in B$ tal que $\varphi(a)b = b\varphi(a), \forall a \in A$, existe un único morfismo de anillos que hace conmutar el siguiente diagrama:*



*donde $\iota : A \to A[x]$ denota la inclusión.*

*Demostración.* Es fácil probar que una función $\hat{\varphi} : A[x] \to B$ es un morfismo de grupos y que verifica $\hat{\varphi}(a) = \varphi(a)\ \forall a \in A$ si y sólo si $\hat{\varphi}\left(\sum_{k=0}^{n} a_i x^i\right) = \sum_{k=0}^{n} \varphi(a_i) b^i$. La condición de que $b$ conmuta con $\mathrm{Im}\,(\varphi)$ asegura la multiplicatividad de $\hat{\varphi}$. □

*Observación* 0.3.2. En el caso particular en que $B$ es conmutativo, la condición de que $b$ conmuta con $\mathrm{Im}\,(\varphi)$ se verifica trivialmente.

**Ejemplo 0.3.1.** Tomando en la proposición anterior $A = \mathbb{Z}, B = \mathbb{R}, \varphi : \mathbb{Z} \to \mathbb{R}$ la inclusión y $b = \sqrt{2}$, tenemos

$$\hat{\varphi}\left(\sum_{k=0}^{n} a_i x^i\right) = \sum_{k=0}^{n} a_i (\sqrt{2})^i.$$

Se tiene $\mathrm{Im}\,(\hat{\varphi}) = \mathbb{Z}[\sqrt{2}]$.

### 0.3.3. Generalización a varias indeterminadas

Si queremos definir el anillo de las series formales en dos variables con coeficientes en $A$, tomamos el conjunto $\{f : \mathbb{N} \times \mathbb{N} \to A\}$, con las operaciones:

$$(f+g)(n,m) = f(n,m) + g(n,m), \qquad (fg)(n,m) = \sum_{\substack{k+l=n \\ q+r=m}} f(k,q)\, g(l,r)$$

Se trabaja análogamente que en el caso de una variable y se nota al anillo obtenido $A[[x,y]]$. Con identificaciones análogas, se obtiene que:

$$A[[x,y]] = \left\{ \sum_{i+j \geqslant 0} a_{ij} x^i y^j \mid a_{ij} \in A \right\}$$

Los polinomios en dos variables con coeficientes en $A$ corresponden al subanillo $A[x,y] = \{f \in A[[x,y]] \mid \sharp\mathrm{sop}(f) < \infty\}$. Con identificaciones análogas, se obtiene que:

$$A[x,y] = \left\{ \sum_{i+j=0}^{n} a_{ij} x^i y^j \mid a_{ij} \in A, n \in \mathbb{N} \right\}$$

Se tiene además que $A[[x,y]] \cong A[[x]][[y]] \cong A[[y]][[x]]$ y que $A[x,y] \cong A[x][y] \cong A[y][x]$. En efecto, las aplicaciones:

| | |
|---|---|
| $\varphi : A[[x,y]] \to A[[x]][[y]]$ | $\psi : A[[x,y]] \to A[[y]][[x]]$ |
| $\varphi(f)(n) \in A[[x]], (\varphi(f)(n))\,(m) = f(m,n)$ | $\psi(f)(n) \in A[y], (\psi(f)(n))\,(m) = f(n,m)$ |

definen isomorfismos de anillos cuyas restricciones a $A[x,y]$ tienen respectivamente por imagen a $A[x][y]$ y $A[y][x]$ (subanillos de $A[[x]][[y]]$ y $A[[y]][[x]]$ respectivamente). Observar por ejemplo que se tiene

$$\begin{aligned} f &= 5 + xy^2 - xy^3 + 3x^2 - 2x^2y^3 \ \in \mathbb{Z}[x,y] \\ &= 5 + (y^2 - y^3)x + (3 - 2y^3)x^2 \ \in \mathbb{Z}[y][x] \\ &= 5 + 3x^2 + xy^2 + (-x - 2x^2)y^3 \in \mathbb{Z}[x][y] \end{aligned}$$

Sin mayor dificultad todo lo anterior puede hacerse para un número $n$ cualquiera de variables considerando el conjunto $A^{\mathbb{N}^n}$.

## 0.4. Ideales

**Definición 0.4.1.** Se considera un anillo $A$ y un subconjunto $I \subseteq A$ tal que $(I,+,0) \leqslant (A,+,0)$. Decimos que:

- $I$ es un *ideal a izquierda* de $A$ si $ax \in I, \forall a \in A, x \in I$. En este caso notamos $I \lhd_l A$,
- $I$ es un *ideal a derecha* de $A$ si $xa \in I, \forall a \in A, x \in I$. En este caso notamos $I \lhd_r A$,
- $I$ es un *ideal bilátero* (o simplemente un *ideal*) de $A$ si $I$ es a la vez ideal izquierdo y derecho de $A$. En este caso notamos $I \lhd A$.

*Observación* 0.4.1.

- Se tiene que $\{0\} \lhd A$ y $A \lhd A$: son los llamados *ideales triviales* de $A$. Los demás ideales se dicen *ideales propios* de $A$.
- Si $I \lhd A$ y $1 \in I$, entonces $I = A$. En particular, $I$ no es un subanillo a menos que $I = A$.
- Un anillo con división no tiene ideales biláteros propios. En efecto, si $I \neq 0$ es un ideal de un anillo con división $A$, tomemos $x \in I, x \neq 0$. Existe $y \in A$ tal que $yx = 1 \in I$, por lo que $I = A$.
- Todas las afirmaciones anteriores valen tomando $\lhd_l$ y $\lhd_r$ en lugar de $\lhd$.

**Ejemplos 0.4.1.**

- **Ideales de $\mathbb{Z}$**
  Son los conjuntos $nZ$ de los múltiplos de $n$, con $n \in \mathbb{N}$ cualquiera.
  En efecto, se puede ver fácilmente que para cada $n \in \mathbb{N}$, $nZ$ es un ideal de $\mathbb{Z}$.
  Por otra parte, si $I$ es un subgrupo de $\mathbb{Z}$, consideremos el menor natural no nulo $n$ que pertenece a $I$. Sea $x \in I$ cualquiera. Vamos a probar que $x$ es múltiplo de $n$. Usando la división entera se tiene $x = qn + r$, con $0 \leqslant r < n$. Como $r = x - qn \in I$ (observar que de $n \in I$ se deduce $qn \in I$ y como además $x \in I$, se tiene $x - qn \in I$), y $r < n$, se deduce $r = 0$ y por lo tanto $x$ es múltiplo de $n$.

- **Ideales y morfismos**
  Si $\varphi : A \to B$ es un morfismo de anillos, entonces $\mathrm{Ker}(\varphi) \lhd A$.

  **Proposición 0.4.1.** *Sea $f : A \to B$ morfismo de anillos. Si $H \lhd B$, entonces $f^{-1}(H) \lhd A$. Si además $f$ es un epimorfismo y $K \lhd A$, entonces $f(K) \lhd B$.*

  *Demostración.* Sea $H \lhd B$. Sabemos que $f^{-1}(H) \leqslant A$. Además, si $x \in f^{-1}(H)$ y $a \in A$ se tiene $f(ax) = f(a)f(x) \in H$ y $f(xa) = f(x)f(a) \in H$ porque $f(x) \in H$. Se deduce que $ax, xa \in f^{-1}(H)$.

  Por otra parte, si $K \lhd A$, sabemos que $f(K) \leqslant B$. Además, si $x \in K$ y $b \in B$, como $f$ es un epimorfismo, se tiene que $b = f(a)$ para algún $a \in A$, de donde $bf(x) = f(a)f(x) = f(ax) \in f(K)$ y $f(x)b = f(x)f(a) = f(xa) \in f(K)$ porque $ax, xa \in K$. □

  Observar que la inclusión de $\mathbb{Z}$ en $\mathbb{R}$ es un morfismo de anillos que muestra que la condición de ser epimorfismo en la proposición anterior es necesaria.

- **Ideales en matrices**
  Para cualquier anillo $A$,

$$\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in A \right\} \lhd_l M_2(A), \qquad \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in A \right\} \lhd_r M_2(A).$$

En $M_2(\mathbb{Z})$, las matrices con todas sus entradas pares forman un ideal bilátero.

En $M_2(\mathbb{R})$, los únicos ideales biláteros son los triviales. En particular, cualquier morfismo de anillos $\varphi : M_2(\mathbb{R}) \to A$ es inyectivo o nulo.

**Proposición 0.4.2.** *Sea $\{J_i\}_{i\in I}$ una familia no vacía de ideales de $A$. Entonces $\bigcap_{i\in I} J_i$ es un ideal de $A$.*

**Definición 0.4.2** (Ideal generado)**.** Si $S \subset A$ es un subconjunto de un anillo, el *ideal bilátero generado por $S$* es:

$$[S] := \bigcap \{I \mid I \lhd A, I \supset S\}$$

Si $S = \{a_1, a_2, \ldots, a_n\}$, notamos $[S] = (a_1, a_2, \cdots, a_n)$. Los ideales generados por un conjunto finito se dicen *finitamente generados*.

Un ideal $(x)$ generado por un conjunto unitario se dice *ideal principal*.

Remplazando $\lhd$ por $\lhd_l$, $\lhd_r$ se define el *ideal a izquierda* o *ideal a derecha* generado por $S$, que se nota $[S]_l$ y $[S]_r$ respectivamente.

*Observación* 0.4.2. El ideal bilátero (a izquierda, a derecha) generado por $S$ es el menor (con respecto a $\subset$) entre los ideales biláteros (a izquierda, a derecha) de $A$ que contienen a $S$. Además se tiene:

$$[S] = \left\{ \sum_{i\in F} a_i s_i b_i \mid F \text{ finito}, a_i, b_i \in A, s_i \in S \ \forall i \in F \right\}$$

$$[S]_l = \left\{ \sum_{i\in F} a_i s_i \mid F \text{ finito}, a_i \in A, s_i \in S \ \forall i \in F \right\}$$

$$[S]_r = \left\{ \sum_{i\in F} s_i b_i \mid F \text{ finito}, b_i \in A, s_i \in S \ \forall i \in F \right\}$$

Es claro que en el caso conmutativo los tres conjuntos coinciden.

La siguiente proposición recoge observaciones ya hechas y las completa.

**Proposición 0.4.3.** *1. Sea $I \lhd A$. Entonces $I = A$ si y sólo si $1 \in I$, si y sólo si existe $x \in U(A)$ tal que $x \in I$.*

*2. Sea $A$ un anillo. Entonces $A$ es un anillo con división si y sólo si $A$ no contiene ideales propios izquierdos ni derechos.*

*3. Sea $A$ un anillo conmutativo. Entonces $A$ es un cuerpo si y sólo si $A$ no tiene ideales biláteros propios.*

*Demostración.* 1. Es claro.

2. Para el directo, ver la observación 0.4.1. Para el recíproco, tomemos $x \in A$, $x \neq 0$ y consideremos el ideal izquierdo $I$ generado por $x$. Como $A$ no tiene ideales propios y además $I \neq 0$, se tiene $I = A$ por lo que $1 \in I$, de donde se deduce que existe $y \in A$ tal que $1 = yx$, por lo que $x$ es invertible a izquierda. Análogamente se prueba que $x$ es invertible a derecha, por lo que $x$ es invertible en $A$.

3. Es la parte anterior aplicada al caso conmutativo. □

**Definición 0.4.3.** Sea $A$ un anillo. Un ideal $M$ bilátero (a izquierda, a derecha) se dice *maximal* si $M \neq A$ y para cualquier otro ideal $J$ bilátero (a izquierda, a derecha) que contiene a $M$ se tiene $J = M$ o $J = A$.

Recordemos el

**Lema de Zorn.** *Sea $(E, \leqslant)$ un conjunto no vacío parcialmente ordenado (i.e. $\leqslant$ es una relación binaria reflexiva, antisimétrica y transitiva) tal que toda cadena $T$ en $E$ (i.e. $T \subset E$ es totalmente ordenado) tiene cota superior en $E$. Entonces $E$ admite un elemento maximal.*

**Teorema 0.4.4.** *Sea $I$ un ideal bilátero (a izquierda, a derecha) de $A$, $I \neq A$. Existe un ideal bilátero (a izquierda, a derecha) maximal $M$ tal que $I \subseteq M$.*

*Demostración.* Haremos la prueba para ideales biláteros, pero es fácilmente adaptable a los casos de ideales a izquierda y a derecha.

Consideremos la familia $\mathcal{F} = \{J \lhd A \mid I \subseteq J \subsetneq A\}$. Como $I \in \mathcal{F}$, se tiene que $\mathcal{F} \neq \varnothing$. Ordenemos $\mathcal{F}$ por inclusión; sea $T = \{I_\lambda \mid \lambda \in \Lambda\} \subseteq \mathcal{F}$ una cadena. Está acotada superiormente por $D := \bigcup_{\lambda \in \Lambda} I_\lambda$. Veamos que $D \in \mathcal{F}$:

- $D \lhd A$: sean $a \in D, b \in D$. Entonces $a \in I_\alpha$, $b \in I_\beta$ para ciertos $\alpha, \beta \in \Lambda$. Como $T$ es una cadena, podemos suponer $I_\alpha \subset I_\beta$, de donde $a, b \in I_\beta$. Esto implica que $a - b \in I_\beta \subset D$. Además $0 \in I_\beta \subset D$, y si $a \in A$, $x \in D$ entonces $x \in I_\gamma$ para algún $\gamma \in \Lambda$, de donde $xa, ax \in I_\gamma \subset D$.
- Como $I \subset I_\lambda$ para todo $\lambda \in \Lambda$, entonces $I \subset D$.
- $D \neq A$: si $D = A$, entonces $1 \in D$, de donde $1 \in I_\lambda$ para algún $\lambda \in \Lambda$, lo cual es absurdo pues $I_\lambda \neq A$.

Aplicando el lema de Zorn a la familia $\mathcal{F}$, se tiene que existe un elemento maximal en $\mathcal{F}$ (ordenado por la inclusión), llamémosle $M \in \mathcal{F}$. Se deduce que $M$ es un ideal maximal en $A$, y por construcción $I \subseteq M$. □

Aplicando el teorema anterior al ideal $I = \{0\}$, se obtiene el siguiente corolario.

**Corolario 0.4.5.** *Si $A \neq \{0\}$ es un anillo, existen ideales biláteros (a izquierda, a derecha) maximales en $A$.*

*Observación* 0.4.3. Se puede demostrar que el teorema anterior (a veces llamado *teorema de Krull*), que usa el axioma de elección bajo la forma del lema de Zorn, es equivalente al axioma de elección. Observar además que usamos fuertemente que nuestro anillo tiene unidad: este teorema es falso para anillos sin unidad.

**Proposición-Definición 0.4.1.** Sean $I, J$ ideales biláteros (a izquierda, a derecha) de $A$. Entonces los siguientes son ideales biláteros (a izquierda, a derecha) de $A$:

- $I + J = \{x + y \mid x \in I, y \in J\}$: es el *ideal suma* de $I$ y $J$,
- $IJ = [\{xy \mid x \in I, y \in J\}] = \left\{ \sum_{k=1}^{n} x_k y_k \mid n \in \mathbb{N}, x_k \in I, y_k \in J, \forall k \in \{1, 2, \cdots, n\} \right\}$: es el *ideal producto* de $I$ y $J$,

*Demostración.* A cargo del lector. □

## 0.5. Anillo cociente

Sean $A$ un anillo e $I \lhd A$. Como $I$ es un subgrupo de $(A, +, 0)$, tiene sentido considerar la relación de congruencia módulo $I$. El siguiente resultado asegura que esta relación es compatible con la estructura multiplicativa de $A$.

**Lema 0.5.1.** *Sean $A$ un anillo e $I \lhd A$. Si $a \equiv a'$ (mód $I$) y $b \equiv b'$ (mód $I$), entonces $ab \equiv a'b'$ (mód $I$).*

*Demostración.* Pongamos $a' = a + i, b' = b + j$ con $i, j \in I$. Se tiene entonces

$$a'b' = (a + i)(b + j) = ab + ib + aj + ij.$$

Como $I \lhd A$, $a'b' - ab = ib + aj + ij \in I$, es decir, $ab \equiv a'b'$ (mód $I$). □

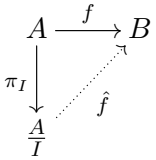
A partir de esto, es inmediato el siguiente resultado.

**Teorema 0.5.2.** *Si $A$ es un anillo e $I \lhd A$, entonces el conjunto $A/_{\equiv}$ con las operaciones*

$$\overline{a} + \overline{b} = \overline{a + b}, \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b} \qquad \forall a, b \in A$$

*y los neutros $\overline{0}$ y $\overline{1}$ forman un anillo que llamamos* anillo cociente de $A$ sobre $I$ *y que notamos $\frac{A}{I}$. Además la proyección canónica $\pi_I : A \to \frac{A}{I}$ es un epimorfismo de anillos.*

**Teorema 0.5.3** (Propiedad Universal del Cociente)**.** *Sea $f : A \to B$ un morfismo de anillos y sea $I \lhd A$. Si $I \leqslant \operatorname{Ker} f$, existe un único morfismo $\hat{f} : \frac{A}{I} \to B$ que hace conmutar el siguiente diagrama:*

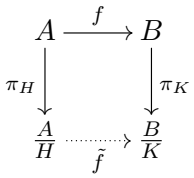



*Además, se tiene* $\operatorname{Im} \hat{f} = \operatorname{Im} f$ *y* $\operatorname{Ker} \hat{f} = \frac{\operatorname{Ker} f}{I}$.

*Demostración.* Sabemos que existe un único morfismo de grupos que hace conmutar el diagrama y verifica las condiciones en el núcleo y la imagen. Es inmediato verificar que dicho morfismo preserva el producto y la unidad del anillo. □

**Corolario 0.5.4** (Teoremas de isomorfismo)**.** *Sea $A$ un anillo.*

1. *Si $f : A \to B$ es un morfismo de anillos, entonces $\frac{A}{\operatorname{Ker} f} \cong \operatorname{Im} f$,*
2. *Si $f : A \to B$ es un morfismo de anillos, y $H \lhd A, K \lhd B$ con $f(H) \subseteq K$, entonces existe un único morfismo de anillos $\tilde{f} : \frac{A}{H} \to \frac{B}{K}$ que hace conmutar el siguiente diagrama:*




*Demostración.* 1. Se deduce del teorema anterior, de manera análoga que para grupos.

2. Sabemos que existe un único morfismo de grupos. Basta verificar que preserva el producto y la unidad. □

**Teorema 0.5.5.** *Sean $A$ un anillo e $I \lhd A$. Existe una correspondencia biyectiva entre los conjuntos:*

$$\mathcal{F}_1 = \left\{ L \lhd \frac{A}{I} \right\} \quad y \quad \mathcal{F}_2 = \{K \lhd A \mid K \supseteq I\}$$

*que preserva la inclusión.*

*Demostración.* La prueba del resultado análogo para grupos puede adaptarse fácilmente a este contexto, usando la proposición 0.4.1. □

Es inmediato el siguiente corolario.

**Corolario 0.5.6.** *Sea $M$ un ideal bilátero de un anillo $A$. Son equivalentes:*

- *$M$ es maximal,*
- *El anillo $\frac{A}{M}$ es no nulo y no tiene ideales biláteros propios (es un anillo* simple*).*

Este último resultado relaciona propiedades del ideal con propiedades del cociente. Vamos a dar otros resultados en este sentido, en el caso de anillos conmutativos, en la siguiente sección.

**Ejemplo 0.5.1.** Sea $A = \mathbb{R}[x], a \in \mathbb{C}$. El *morfismo de evaluación en $a$* es $\varepsilon_a : \mathbb{R}[x] \to \mathbb{C}$, $\varepsilon_a(f) = f(a)$.

Supongamos $a \in \mathbb{R}$. Entonces se tiene que Im $\varepsilon_a = \mathbb{R}$ y que

$$\operatorname{Ker} \varepsilon_a = \{f \in \mathbb{R}[x] : f(a) = 0\} \ni X - a.$$

Por otro lado $f(a) = 0 \Leftrightarrow f = (x-a)q$ para algún $q \in \mathbb{R}[x]$. En conclusión $\operatorname{Ker} \varepsilon_a = (x-a)$. Por el primer teorema de isomorfismo concluimos que $\frac{\mathbb{R}[x]}{(x-a)} \cong \mathbb{R}$ que es un cuerpo.

Tomemos ahora $a = i$, la unidad imaginaria. Entonces $\varepsilon_i$ es un epimorfismo: dado $a + ib \in \mathbb{C}$ basta tomar $f = a + bX$. Se tiene que

$$\operatorname{Ker} \varepsilon_i = \{f \in \mathbb{R}[x] : f(i) = 0\} \ni X^2 + 1.$$

y que Im $\varepsilon_i = \mathbb{C}$. Por otro lado $f(i) = 0 \Rightarrow f(-i) = 0 \Rightarrow f$ es divisible por $(x+i)(x-i) = x^2 + 1$. En conclusión $\operatorname{Ker} \varepsilon_i = (X^2 + 1)$. Por el primer teorema de isomorfismo concluimos que $\mathbb{C} \cong \frac{\mathbb{R}[x]}{(X^2+1)}$. Esta es una construcción algebraica de los números complejos.

## 0.6. Ideales maximales e ideales primos

**Definición 0.6.1.** Sea $A$ un anillo conmutativo. Un ideal $P$ de $A$ se dice *primo* si $P \neq A$ y

$$\forall a, b \in A : ab \in P \Rightarrow a \in P \text{ o } b \in P.$$

**Ejemplos 0.6.1** (Ideales primos)**.** 1. $p\mathbb{Z} \lhd \mathbb{Z}$ es primo. Más aún, son equivalentes para un entero positivo $m$:

(i) $m\mathbb{Z}$ es primo,

(ii) $m\mathbb{Z}$ es maximal,

(iii) $m$ es un número primo.

Tenemos (iii) implica (i) y (iii) implica (ii). Para los recíprocos, supongamos que $m$ no es primo. Se tiene entonces $m = ab, a, b \notin \{1, -1\}$. Entonces $(m) \subsetneq (a)$ por lo que no vale (ii) y además $a, b \notin m\mathbb{Z}$ mientras que $ab \in n\mathbb{Z}$, por lo que no vale (i).

2. si $D \neq \{0\}$ es un dominio, el ideal $\{0\}$ es primo,

3. si $D$ es un dominio, entonces $(x, y) = \{p \in D[x, y] \mid p(0) = 0\} \lhd D[x, y]$ es un ideal primo.

**Proposición 0.6.1.** *Sean $A$ un anillo conmutativo e $I \lhd A$. Entonces:*

1. *$I$ es maximal si y sólo si $\frac{A}{I}$ es cuerpo,*

2. *$I$ es primo si y sólo si $\frac{A}{I}$ es dominio.*

*Demostración.* 1. Esta parte puede deducirse fácilmente combinando los dos resultados que siguen en el caso de anillos conmutativos:

- $I$ es maximal si y sólo si $\frac{A}{I}$ no tiene ideales biláteros (corolario 0.5.6),
- $B$ es un anillo con división si y sólo si no tiene ideales a izquierda ni a derecha (proposición 0.4.3).

Sin embargo, presentamos una prueba autocontenida para ejercitar la manipulación con ideales maximales y con anillos cociente:
($\Rightarrow$) Sea $\overline{a} \in \frac{A}{I}$ tal que $\overline{a} \neq 0$. Veamos que es invertible.

Como $a \notin I$, se tiene que $I \subsetneq I + (a) = \{x + ay : x \in I, y \in A\}$. Como $I$ es maximal, esto implica que $I + (a) = A$. En particular $A \ni 1 = x + ay$ para ciertos $x \in I, y \in A$. Por lo tanto $ay - 1 \in I$, es decir, $\overline{ay} = \overline{1} = \overline{ya}$.

($\Leftarrow$) Si $\frac{A}{I}$ es un cuerpo, entonces sus únicos ideales son $\{0\}$ y $\frac{A}{I}$. El teorema de correspondencia 0.5.5 nos indica que estos están en biyección con los ideales de $A$ que contienen a $I$, entre los cuales necesariamente están $I$ y $A$, por lo tanto no puede haber más. Esto nos dice exactamente que $I$ es maximal.

2. ($\Rightarrow$) Sean $\overline{a}, \overline{b} \in \frac{A}{I}$ tales que $\overline{a}\overline{b} = \overline{ab} = \overline{0}$. Entonces $ab \in I$. Como $I$ es primo esto implica que $a \in I$ o $b \in I$, es decir, $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$, probando que $\frac{A}{I}$ es un dominio.

($\Leftarrow$) Sea $ab \in I$. Entonces $\overline{0} = \overline{ab} = \overline{a}\overline{b}$. Como $\frac{A}{I}$ es dominio, esto implica que $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$, es decir $a \in I$ o $b \in I$, de donde $I$ es un ideal primo. □

Se deduce el siguiente corolario.

**Corolario 0.6.2.** *Sea $A$ un anillo conmutativo.*

1. *Todo ideal maximal en $A$ es primo.*

2. *Si $\varphi : A \to B$ un morfismo de anillos, entonces* $\operatorname{Ker} \varphi$ *es maximal si y sólo si* $\operatorname{Im} \varphi$ *es un cuerpo, y* $\operatorname{Ker} \varphi$ *es primo si y sólo si* $\operatorname{Im} \varphi$ *es un dominio.*

*Observación* 0.6.1. A partir de los resultados anteriores y del ejemplo 0.6.1, se tiene:

- Sea $m \in \mathbb{Z}$. Son equivalentes:

  (i) $\mathbb{Z}_m$ es un cuerpo,

  (ii) $\mathbb{Z}_m$ es un dominio,

  (iii) $m$ es un número primo.

- Si consideramos el morfismo $\varphi_n : \mathbb{Z}[x] \to \mathbb{Z}$ tal que $(\varphi_n)_{|\mathbb{Z}} = \mathrm{id}_{\mathbb{Z}}$ y $\varphi_n(x) = n$, como $\mathrm{Im}\,\varphi_n = \mathbb{Z}$ es un dominio que no es un cuerpo, se deduce que $\mathrm{Ker}\,\varphi_n \lhd \mathbb{Z}[x]$ es un ideal primo que no es maximal. En particular $\mathrm{Ker}\,\varphi_0 = (x) = \{p \in \mathbb{Z}[x] \mid p(0) = 0\}$ es un ideal primo no maximal. En efecto, $(x) \subsetneq \{p \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z}\}$.

- Sea $\Bbbk$ un cuerpo. Para cada $\alpha \in \Bbbk$, el ideal $I_\alpha = (x - \alpha)$ es maximal en $\Bbbk[x]$. (Veremos más adelante que hay ideales maximales que no son de la forma $I_\alpha$).

- Sea $\Bbbk$ un cuerpo. El único ideal maximal de $\Bbbk[[x]]$ es $(x)$. En efecto, supongamos que $M$ es maximal. Observemos primero que si $f \in \Bbbk[[x]]$ es tal que $f(0) \neq 0$, entonces $f$ es invertible. Es claro entonces que $\forall f \in M$ se tiene $f(0) = 0$, entonces todo $f \in M$ es de la forma $f = gx$ y por tanto $M \subseteq (x) \subsetneq \Bbbk[[x]]$ es decir $M = (x)$.

*Observación* 0.6.2. Sea $A$ un anillo. Llamémosle $\chi$ al único morfismo de anillos $\mathbb{Z} \to A$, es decir $\chi(n) = n \cdot 1_A = \overbrace{1_A + \cdots + 1_A}^{n \text{ veces}}$. El núcleo de $\chi$ es $\mathrm{Ker}\,\chi = \{n \in \mathbb{Z} : n \cdot 1_A = 0\} = m\mathbb{Z}$ para algún $m \in \mathbb{N}$.[2] Definimos la *característica* de $A$ como $m$. Notamos $\mathrm{car}\, A = m$. A modo de ejemplo, el único anillo de característica 1 es el anillo trivial $\{0\}$.

El primer teorema de isomorfismo afirma que $\frac{\mathbb{Z}}{m\mathbb{Z}} \simeq \mathrm{Im}\,\chi \subset A$. Observar que si $\varphi : R \to S$ es un morfismo de anillos y $R$ es un anillo conmutativo, entonces $\mathrm{Im}\,\varphi$ es un subanillo conmutativo de $B$. En este caso tenemos que $\mathrm{Im}\,\chi \subset A$ es un subanillo conmutativo.

Si además $A$ no tiene divisores de cero ni a izquierda ni a derecha (por ejemplo, si $A$ es un dominio o un anillo con división), entonces $\mathrm{Im}\,\chi$ tampoco tendrá. En este caso $\frac{\mathbb{Z}}{m\mathbb{Z}}$ es un dominio, de donde $m\mathbb{Z}$ es un ideal primo. En conclusión, $m = 0$ o $m = p$ es un número primo.

En particular, un cuerpo tiene característica cero o característica prima.

## 0.7. Anillos de fracciones y localización

Los números racionales pueden construirse de manera algebraica a partir de los enteros de la siguiente manera: se considera el conjunto $\mathbb{Z} \times \mathbb{Z}\backslash\{0\} = \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}$ y se define la relación:

$$(a, b) \sim (c, d) \text{ si y sólo si } ad = bc.$$

A partir de la conmutatividad y la ausencia de divisores de cero en $\mathbb{Z}$, se prueba que esta relación es de equivalencia y se nota $\frac{a}{b}$ a la clase del elemento $(a, b)$ y $\mathbb{Q}$ al conjunto cociente. La idea es que $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$ permite definir un racional como un par de enteros, con el segundo no nulo.

La aplicación que asocia a cada entero $n$ el par $(n, 1) \in \mathbb{Q}$ es una función inyectiva. Se quiere dar a $\mathbb{Q}$ una estructura de anillo que sea coherente con la estructura de anillo de $\mathbb{Z}$ (esto es, una estructura tal que la inyección antes mencionada sea un morfismo de anillos). Para esto se define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \bullet \frac{c}{d} = \frac{ac}{bd}$$

y se prueba que $(\mathbb{Q}, +, \frac{0}{1}, \bullet, \frac{1}{1})$ es un cuerpo.

Esta construcción puede generalizarse en dos etapas:

1. se puede considerar en lugar de $\mathbb{Z}$ un dominio cualquiera $A$ y dar una estructura de cuerpo a un cociente del conjunto $A \times A\backslash\{0\}$: este cuerpo se llama *cuerpo de fracciones* de $A$,

[2] De manera equivalente se define la característica del anillo como el menor $n$ positivo tal que $n \cdot 1_A = 0$ si existe, o como 0 si no existe.

2. en la construcción del cuerpo de fracciones se toman todos los elementos no nulos de $A$ y se transforman en invertibles: una construcción más general permite transformar en invertibles los elementos de un *subconjunto multiplicativo* $S$ de un anillo conmutativo $A$, mediante un proceso cuyo resultado no es necesariamente un cuerpo sino un anillo conmutativo llamado *anillo de fracciones de $A$ respecto de $S$*.

La construcción del cuerpo de fracciones a partir de un dominio $A$ es análoga a la de $\mathbb{Q}$ a partir de $\mathbb{Z}$. Vamos a concentrarnos en la segunda etapa y luego ver al cuerpo de fracciones como un caso particular de anillo de fracciones.

**Definición 0.7.1.** Sea $A$ un anillo conmutativo. Un conjunto $S \subseteq A$ se dice *multiplicativo* o *multiplicativamente cerrado* si $1 \in S$ y $st \in S \ \ \forall s, t \in S$.

**Ejemplos 0.7.1** (Conjuntos multiplicativos)**.** 1. $\{1\}$, $A$ son conjuntos multiplicativos en $A$,

2. para cada $a \in A$, el conjunto $\{a^n \mid n \in \mathbb{N}\}$ es multiplicativo en $A$,

3. si $P$ es un ideal primo de $A$, el conjunto $S = A \backslash P$ es multiplicativo,

4. en particular, si $A$ es un dominio, $A\backslash\{0\}$ es multiplicativo.

Definimos en $A \times S$ la siguiente relación:

$$(a, s) \sim_S (b, r) \text{ si y sólo si existe } t \in S \text{ tal que } t(ar - bs) = 0.$$

Notamos $\frac{a}{s}$ a la clase de equivalencia del par $(a, s)$.

*Observación* 0.7.1. 1. Sean $A$ un anillo conmutativo y $S$ un conjunto multiplicativo en $A$. La relación $\sim_S$ definida en $A \times S$ es de equivalencia. En efecto, es reflexiva porque $(a, s) \sim_S (a, s)$ se verifica tomando $t = 1 \in S$ y usando la conmutatividad de $A$. La relación es simétrica porque $A$ es conmutativo. Para la transitividad, supongamos $(a, s) \sim_S (b, r)$ y $(b, r) \sim_S (c, v)$. Existen $t, t' \in S$ tales que $t(ar - bs) = 0$ y $t'(bv - cr) = 0$. Se tiene que $tt'rav = tt'bsv = tt'crs$ de donde $tt'r(av - cs) = 0$. Como $t, t', r \in S$ se tiene que $tt'r \in S$, de donde $(a, s) \sim_S (c, v)$.

2. Se tiene que $\frac{a}{s} = \frac{at}{st} \ \ \forall a \in A, s, t \in S$.

3. Si $A$ es un dominio y $0 \notin S$, la relación puede expresarse como $(a, s) \sim_S (b, t)$ si y sólo si $at = bs$.

**Proposición-Definición 0.7.1.** Sean $A$ un anillo conmutativo y $S$ un conjunto multiplicativo en $A$. El conjunto cociente $\frac{A \times S}{\sim_S}$ admite una estructura de anillo conmutativo que llamamos *anillo de fracciones* (o *de localización*) de $A$ respecto de $S$ y notamos $S^{-1}A$, cuyas operaciones se definen como sigue:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s} \bullet \frac{b}{t} = \frac{ab}{st}, \qquad \forall a, b \in A, s, t \in S.$$

*Demostración.* Verifiquemos primero que las operaciones están bien definidas. Para $+$, es claro por la conmutatividad de la suma y el producto en $A$ que alcanza con probar que si $\frac{a}{s} = \frac{a'}{s'}$ entonces $\frac{at+bs}{st} = \frac{a't+bs'}{s't}$ para todo $b \in A, t \in S$. Ahora bien, si existe $x \in S$ tal que $xas' = xa's$, entonces

$$x(at + bs)(s't) = xas't^2 + xbs'st = xa'st^2 + xbs'st = xst(a't + bs')$$

y se deduce la igualdad.

Análogamente, para $\bullet$ alcanza con observar que si $\frac{a}{s} = \frac{a'}{s'}$ entonces $\frac{a'b}{s't} = \frac{ab}{st}$ para todo $b \in A, t \in S$. La implicancia es inmediata puesto que $xas' = xa's$ implica $xas'bt = xa'sbt$.

Veamos ahora que $+$ define una estructura de grupo abeliano. La conmutatividad es clara. La asociatividad se deduce de:

$$\frac{(at+bs)r+cst}{str} = \frac{atr+(br+ct)s}{str} \quad \forall a,b,c \in A, s,t,r \in S.$$

Se tiene además $\frac{a}{s}+\frac{0}{1} = \frac{a\cdot 1+s\cdot 0}{s\cdot 1} = \frac{a}{s}$ y $\frac{-a}{s}+\frac{a}{s} = \frac{0}{s^2} = \frac{0}{1}$, $\forall a \in A, s \in S$.

La operación $\bullet$ es claramente asociativa y conmutativa y $\frac{1}{1}$ es su neutro.

Finalmente, para verificar que el producto es distributivo respecto de la suma, es decir que se cumple

$$\frac{a}{s} \bullet \left(\frac{b}{t}+\frac{c}{r}\right) = \frac{ab}{st}+\frac{ac}{sr} \quad \forall a,b,c \in A, s,t,r \in S.$$

observemos que el término de la izquierda de la igualdad es $\frac{a}{s} \bullet \frac{br+ct}{tr} = \frac{a(br+ct)}{str}$ y el de la derecha es $\frac{absr+acst}{s^2tr} = \frac{abr+act}{str}$. □

*Observación* 0.7.2. Si $0 \in S$, entonces $\frac{a}{s} = \frac{0}{1}$ $\forall a \in A, s \in S$, y por tanto $S^{-1}A = \{0\}$.

Veamos ahora como se relacionan el anillo original $A$ con el anillo de fracciones $S^{-1}A$.

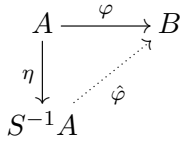
**Proposición 0.7.1.** *Sean $A$ un anillo conmutativo y $S$ un conjunto multiplicativo en $A$. La función*

$$\begin{aligned} \eta_S : A &\to S^{-1}A \\ a &\mapsto \frac{a}{1} \end{aligned}$$

*es un morfismo de anillos.*

*Demostración.* A cargo del lector. □

**Proposición 0.7.2** (Propiedad universal del anillo de fracciones)**.** *Sean $A$ un anillo conmutativo y $S \subset A$ un conjunto multiplicativo. Si $\varphi : A \to B$ es un morfismo de anillos, donde $B$ es un anillo conmutativo tal que $\varphi(S) \subset B^\times$, entonces existe un único morfismo de anillos $\hat{\varphi} : S^{-1}A \to B$ que hace conmutar el siguiente diagrama:*




*Demostración.* A cargo del lector (haremos la demostración de un caso particular en la proposición 0.7.4). □

*Observación* 0.7.3. Supongamos que $0 \notin S$.

- El morfismo $\eta_S$ es inyectivo si y sólo si $S$ no tiene divisores de cero. En efecto, sea $a \in A$ tal que $\eta_S(a) = 0$. Entonces $\frac{a}{1} = \frac{0}{1}$ lo que implica que existe $s \in S$ tal que $as = 0$. Como $s \neq 0$ y $S$ no tiene divisores de cero, se deduce $a = 0$. Recíprocamente, si $s \in S$ es un divisor de cero, existe $a \in A$ tal que $as = 0$ y $a \neq 0$. Se deduce $\eta_S(a) = 0$ y por lo tanto que $\eta_S$ no es inyectiva.

- En particular, si $A$ es un dominio, entonces $\eta_S$ es inyectiva si y sólo si $0 \notin S$.

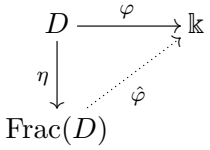
**Proposición 0.7.3.** *$\eta_S$ es un isomorfismo si y sólo si todos los elementos de $S$ son invertibles en $A$.*

*Demostración.* Es claro que si todos sus elementos son invertibles, $S$ no tiene divisores de cero y por lo tanto se tiene que $\eta_S$ es inyectiva. Además, $\forall a \in A, s \in S : \frac{a}{s} = \frac{s^{-1}a}{1} = \eta_S(s^{-1}a)$, por lo que se tiene también la sobreyectividad. Recíprocamente, si $\eta_S$ es sobreyectiva, $\forall s \in S$, existe $a \in A$ tal que $\frac{1}{s} = \frac{a}{1}$, por lo que existe $t \in S$ tal que $t = ast$. Se deduce $\frac{1}{1} = \frac{as}{1}$ de donde $1 = as$ y por lo tanto $s$ es invertible. □

**Proposición-Definición 0.7.2.** Sean $A$ un dominio y $S = A\backslash\{0\}$. El anillo de fracciones $S^{-1}A$ es un cuerpo que llamamos *cuerpo de fracciones de $A$* y notamos $\mathrm{Frac}(A)$. Notaremos $\eta$ al monomorfismo canónico $A \to \mathrm{Frac}(A)$.

*Demostración.* Si $\frac{a}{s} \neq 0$, entonces no existe $t \in S$ tal que $ta = 0$. En particular $a = 1 \cdot a \neq 0$, por lo que $a \in S$ y $\frac{s}{a}$ es el inverso de $\frac{a}{s}$. □

**Proposición 0.7.4** (Propiedad universal del cuerpo de fracciones)**.** *Sea $D$ un dominio. Para cada cuerpo $\Bbbk$ y cada monomorfismo de anillos $\varphi : D \to \Bbbk$ existe un único morfismo de anillos $\hat{\varphi} : \mathrm{Frac}(D) \to \Bbbk$ que hace conmutar el siguiente diagrama:*




*Demostración.* Para la existencia, alcanza con definir

$$\hat{\varphi}\left(\frac{a}{b}\right) := \varphi(a)\varphi(b)^{-1}, \forall a, b \in A, b \neq 0 \quad (*)$$

(notar que si $b \neq 0$ entonces $\varphi(b) \neq 0$ y por tanto es invertible en $\Bbbk$) y probar que es un morfismo de anillos que hace conmutar el diagrama.

Para la unicidad basta ver que la condición de conmutatividad del diagrama es $\hat{\varphi}(\frac{a}{1}) = \varphi(a)\ \ \forall a \in A$ y la condición de que $\hat{\varphi}$ es morfismo de anillos implica $\hat{\varphi}(\frac{1}{b}) = \varphi(b)^{-1}$ $\forall b \in A, b \neq 0$. Combinando ambas igualdades y usando que $\hat{\varphi}$ preserva el producto, se deduce que $\hat{\varphi}$ tiene que estar definida por la fórmula $(*)$. □

**Ejemplos 0.7.2** (Cuerpos de fracciones)**.** Sea $\Bbbk$ un cuerpo.

1. $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ (ver observación 0.7.1.4),
2. $\mathrm{Frac}(\Bbbk) = \Bbbk$.
3. Se define el anillo de las *funciones racionales* con coeficientes en $\Bbbk$ en indeterminadas $x_1, \ldots, x_n$ como

$$\Bbbk(x_1, \ldots, x_n) := \mathrm{Frac}(\Bbbk[x_1, \ldots, x_n]) = \left\{ \frac{f}{g} \mid f, g \in \Bbbk[x_1, \ldots, x_n], g \neq 0 \right\},$$

4. Se define el anillo de las *series de Laurent formales* como

$$\Bbbk((x)) := \mathrm{Frac}\left(\Bbbk[[x]]\right) = \left\{ \frac{f}{g} \mid f, g \in \Bbbk[[x]], g \neq 0 \right\} = \left\{ \frac{h}{x^n} \mid h \in \Bbbk[[x]], n \in \mathbb{N} \right\}.$$

La última igualdad se prueba usando que todo $g \in \Bbbk[x]$ no nulo es de la forma $g = x^n g_1$ para cierto natural $n$ y cierto $g_1 \in \Bbbk[[x]]$ invertible. Análogamente se define $\Bbbk((x_1, \ldots, x_n))$ como el cuerpo de fracciones del anillo de series en las variables $x_1, x_2, \cdots, x_n$.

En el caso particular en que el conjunto multiplicativo $S$ es el complemento de un ideal primo $P$, el proceso se llama de *localización respecto del ideal* $P$. La construcción del cuerpo de fracciones de un dominio es un caso particular de localización respecto de un ideal (considerando $P = \{0\}$).

**Definición 0.7.2.** Si $A$ es un anillo conmutativo y $P$ es un ideal primo en $A$, llamamos *localización de* $A$ *respecto de* $P$ y notamos $A_{(P)}$ al anillo de fracciones $S^{-1}A$, donde $S = A \backslash P$.

**Definición 0.7.3.** Un anillo conmutativo se dice *local* si tiene un único ideal maximal.

**Ejemplos 0.7.3.** Todo cuerpo es un anillo local.
Vamos a ver que la construcción del anillo de fracciones permite obtener anillos locales a partir de ideales primos.
El anillo de series formales en $x$ con coeficientes en un cuerpo es local (su único ideal maximal es $(x)$. Ver ejercicio del repartido 4 al respecto).

**Proposición 0.7.5.** *Sea $A$ un anillo conmutativo no trivial. Son equivalentes:*

1. *$A$ es local,*
2. *la suma de dos elementos no invertibles es no invertible,*
3. *$A \backslash A^\times$ es un ideal de $A$.*

*Demostración.* $(1 \Rightarrow 2)$ Supongamos que $A$ es local y que $M$ es su ideal maximal. Si $x, y \notin A^\times$ entonces existe un ideal maximal que contiene a $x$ y otro que contiene a $y$. Como hay un único ideal maximal, se tiene $x, y \in M$ y por tanto $x + y \in M$. Como $M \neq A$, se deduce que $x + y$ es no invertible.

$(2 \Rightarrow 3)$ Sabemos que $A \backslash A^\times$ es no vacío (porque $A$ es no trivial) y cerrado por la suma. Por otra parte si $x$ es no invertible, también lo es $-x$. Además, si $x$ es no invertible, es claro que $ax$ es no invertible para cualquier $a \in A$. Se deduce que $A \backslash A^\times \lhd A$.

$(3 \Rightarrow 1)$ Es claro que cualquier ideal propio de $A$ está formado por elementos no invertibles, es decir que está contenido en $A \backslash A^\times$. Como consecuencia, si $A \backslash A^\times$ es un ideal, entonces es el único ideal maximal. □

**Proposición 0.7.6.** *Dado $A$ un anillo conmutativo y $P$ un ideal primo de $A$, el anillo $A_{(P)}$ es local y su único ideal maximal es $S^{-1}P := \{\frac{p}{s} \mid p \in P, s \notin P\}$.*

*Demostración.* Es claro que $S^{-1}P$ es un ideal de $A_{(P)}$. Además, su complemento consiste de los elementos de la forma $\frac{t}{s}$ con $t, s \in S$, y por tanto consiste de elementos invertibles. Se deduce por la proposición anterior que $S^{-1}P$ es el único ideal maximal de $A_{(P)}$. □

**Ejemplo 0.7.1.** Tomemos $p\mathbb{Z} \lhd \mathbb{Z}$, siendo $p \in \mathbb{Z}$ primo. La localización de $\mathbb{Z}$ respecto de $p\mathbb{Z}$ es el subanillo

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid b \text{ no es múltiplo de } p \right\} \subseteq \mathbb{Q}.$$

Su único ideal maximal es $\left\{ \frac{a}{b} \mid a \text{ es múltiplo de } p, b \text{ no es múltiplo de } p \right\}$.