Estructuras Básicas del Álgebra

Índice general

Capítulo 1

Conceptos Básicos

Objetivos del capítulo

- Introducir los conceptos básicos de la Teoría de conjuntos. Estudiar las operaciones entre conjuntos y sus propiedades.
- Estudiar el concepto de aplicación. Aplicaciones inyectivas, sobreyectivas, biyectivas. Composición de aplicaciones. Aplicación inversible y caracterizaciones.
- Estudio de las relaciones de equivalencia y su relación con las particiones. Estudio de las relaciones de orden y sus elementos notables.
- Nociones básicas sobre cardinales.

---

1. Conjuntos.

Toda teoría matemática consta de axiomas, o elementos primitivos, a partir de estos se construyen las definiciones. Las relaciones "lógicas" entre definiciones dan lugar a los teoremas (Lema, Proposición, Teorema y Corolario). Comenzamos este capítulo con la noción de conjunto.

1.1. Definiciones básicas.

Conceptos A Un **conjunto** es una colección de objetos. Para construir o crear un conjunto damos explícitamente cada uno de sus elementos o bien damos una propiedad que caracterice a dichos elementos.

⋆ Hasta que no se han dado o caracterizados los elementos de un conjunto, este no es, por lo que la propiedad que determina a los elementos de un conjunto no debe de hacer uso del conjunto en sí. Esta propiedad, como puede verse en el ejercicio 40 (Pag. 50), puede ser algo escurridiza.

⋆ Por la misma razón, un conjunto no puede ser elemento de si mismo (para incluirlo como elemento tiene que ser algo y un conjunto no es algo hasta que se fijan todos sus elementos).

Definición 1 Diremos que un elemento "a" **pertenece** a un conjunto X, y lo denotaremos por $a \in X$, si a es uno de los miembros de X. Si a no es miembro de X diremos que a **no pertenece** a X y lo denotaremos por $a \notin X$.

Nota: Para que un conjunto esté correctamente definido debe de poderse determinar si un objeto pertenece o no pertenece a él de forma inequívoca.
Notación: Los conjuntos los denotaremos por letras mayúsculas mientras que los elementos serán denotados por letras minúsculas.

Ejemplos B

⋆ El conjunto de los números naturales, $\mathbb{N}$.

⋆ El conjunto de los números naturales que son pares.

⋆ $A =: \{1, 2, a\}; B =: \{a, b, c\}; C =: \{2, 3, 5, 7, 11\}$.

⋆ $Y =: \{n \in \mathbb{N} \mid \frac{n}{2} \in \mathbb{N}\}$.

⋆ $X =: \{1, 2, 3, \{1, c\}, \{a\}, b\}$. En este caso, algunos de los elementos de este conjunto son a su vez conjuntos. Esto nos puede llevar a cierta confusión a la hora de saber si un elemento pertenece o no a un conjunto. Así, en este ejemplo,

$$1, b, \{1, c\} \in X, \quad \text{pero} \quad a, c, \{1\}, \{2\} \notin X$$

Hacer hincapié cada vez que se introduzca notación matemática (en Y).

Definición 2 Sean X e Y dos conjuntos:

• Diremos que X es un **subconjunto** de Y, y lo representaremos por $X \subset Y$, que se leerá X contenido en Y, si todo elemento de X es elemento de Y, es decir,

$$X \subset Y \quad \overset{*}{\Longleftrightarrow} \quad \forall^{\dagger} a \in X, \Rightarrow^{\ddagger} a \in Y$$

En caso contrario, cuando X no sea subconjunto de Y (lo que significa que hay un elemento de X que no es elemento de Y) se denotará por $X \not\subset Y$.

• Diremos que X es **igual** a Y, y lo representaremos $X = Y$, si

$$X \subset Y \text{ e } Y \subset X.$$

Denotaremos por $X \neq Y$ cuando X **no** sea **igual** que Y.

• Diremos que X está **estrictamente contenido** en Y, y lo denotaremos $X \subsetneq Y$ si

$$X \subset Y \text{ y } X \neq Y.$$

• Definimos el **conjunto vacío**, denotado por $\emptyset$, como aquél que carece de elementos.

• Definimos el **conjunto partes de** X, y lo representamos por $\mathcal{P}(X)$ como el conjunto que tiene por elementos los subconjuntos de X.

*Relación lógica $\Longleftrightarrow$: establece que las proposiciones a izquierda y derecha de ella son o ambas falsas o ambas verdaderas. A veces es usada para dar una definición

†$\forall$: se lee para todo

‡Relación lógica $\Rightarrow$: establece que si la proposición de la izquierda es verdadera, la de la derecha también lo es

Nota: Observar que de la igualdad de conjuntos se deduce que no importa el "orden" en el que se encuentren colocados los elementos de un conjunto. Así, el conjunto $\{a, b, c\}$ es el mismo que el conjunto $\{c, a, b\}$.

Aunque parezcan nociones fáciles tienen su pega. Poner un conjunto y preguntar que pertenece y que está contenido. Estas nociones tienen que quedar completamente claras.

Ejemplos C

$\star$ Las nociones de pertenece y contenido, aunque fáciles pueden llegar a confundirnos. Sea $X = \{1, \{1\}, \{1, a\}, \{a\}\}$. Entonces

$$1, \{a\} \in X, \quad a \notin X, \quad \{1\}, \{\{a\}\} \subset X, \quad \{1, a\} \not\subset X$$

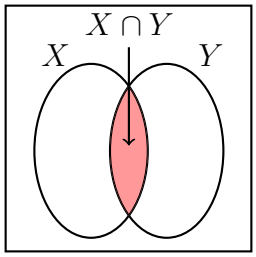
Observar que en este ejemplo $\{1\} \in X$ y $\{1\} \subset X$.

$\star$ Para $A = \{1, 2, a\}$, se tiene que

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{a\}, \{1, 2\}, \{1, a\}, \{2, a\}, \{1, 2, a\}\}.$$

1.2. Operaciones con conjuntos

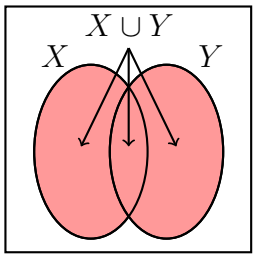
Vamos a definir varios conceptos: (i) cual es la idea, el concepto que queremos definir. (ii) como se define matemáticamente (un poco en la notación matemática de las definiciones). (iii) como se representan por diagramas de Venn (Pueden que no hayan visto nunca representados los conjuntos como diagramas de Venn.)



Definición 3 Dados dos conjuntos X, Y, se define la **intersección** de X con Y y se representa por $X \cap Y$ a un nuevo conjunto que tiene los elementos que están tanto en X como en Y.

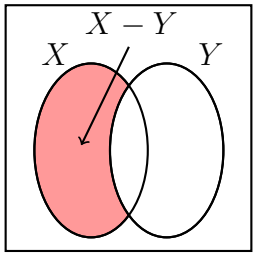
$$X \cap Y = \{z \mid z \in X \text{ y } z \in Y\}$$

Nota: Diremos que dos conjuntos X, Y son **disjuntos** si $X \cap Y = \emptyset$.



Definición 4 Dados dos conjuntos X, Y, se define la **unión** de X con Y y se representa por $X \cup Y$ a un nuevo conjunto que tiene por elementos tanto los elementos de X como los de Y.

$$X \cup Y = \{z \mid z \in X \text{ ó } z \in Y\}$$

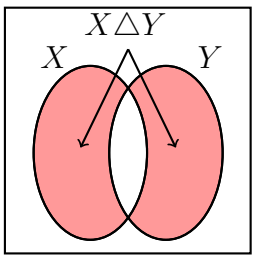


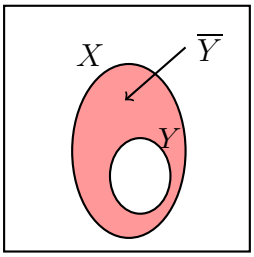
Definición 5 Dados dos conjuntos X, Y, se define la **diferencia** de X con Y y se representa por $X - Y$ al conjunto formado por los elementos de X que no están en Y. Es decir,

$$X - Y = \{z \in X \mid z \notin Y\}$$

Definición 6 Dados dos conjuntos X, Y, se define la **diferencia simétrica** de X con Y y se representa por $X\triangle Y$ al conjunto formado por los elementos de X que no están en Y junto con los de Y que no están en X.

$$X\triangle Y = (X \cup Y) - (Y \cap X) = (X - Y) \cup (Y - X)$$





Definición 7 Dados dos conjuntos X, Y, con X subconjunto de Y se define el **complemento** de X en Y y se representa por $\overline{X}$ al conjunto formado por los elementos de Y que no están en X. Es decir,

$$\overline{X} = \{z \in Y \mid z \notin X\}$$

Definición 8 Dados dos conjuntos X, Y se define el **producto cartesiano** de X e Y y se representa por $X \times Y$ como un nuevo conjunto formado por todos los pares (x, y) en donde $x \in X$ e $y \in Y$.

$$X \times Y := \{(x, y) \mid x \in X \text{ e } y \in Y\}$$

Ejemplos D Dados $A = \{1, 2, a\}$ y $B = \{a, b, c\}$ se tiene que

$$A \times B := \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (a, a), (a, b), (a, c)\}$$

Nota: Los conjuntos $X \times Y$ e $Y \times X$ son distintos siempre que $X \neq Y$.

Es la primera demostración que se les hace

Fin de clase primera 27-09-2011, grupo A y B

Proposición 9 Sean X, Y, Z tres conjuntos. Entonces:

(i) Propiedad Conmutativa: $X \cup Y = Y \cup X$; $\quad X \cap Y = Y \cap X$.

(ii) Propiedad asociativa: $(X \cup Y) \cup Z = X \cup (Y \cup Z)$
$(X \cap Y) \cap Z = X \cap (Y \cap Z)$.

(iii) Propiedad distributiva: $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$
$(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$
$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$.

(iv) Propiedad Idempotente: $X \cup X = X$; $\quad X \cap X = X$.

(v) Leyes de simplificación: $(X \cup Y) \cap X = X$; $\quad (X \cap Y) \cup X = X$.

(vi) Leyes de Morgan: supongamos que X, Y son subconjuntos de un conjunto T, entonces:

$$\overline{(X \cup Y)} = \overline{X} \cap \overline{Y}; \quad \overline{(X \cap Y)} = \overline{X} \cup \overline{Y}.$$

Demo: (i) Demostremos que $X \cup Y = Y \cup X$. Para ello tenemos que demostrar que $X \cup Y \subset Y \cup X$ y que $Y \cup X \subset X \cup Y$. Veamos el primer contenido:

Sea $a \in X \cup Y$ tenemos, por definición de unión de conjuntos que $a \in X$ o $a \in Y$. Por tanto, $a \in Y \cup X$. El otro contenido es igual.

(ii). Demostremos que $(X \cup Y) \cup Z = X \cup (Y \cup Z)$. Sea $a \in (X \cup Y) \cup Z$. Por la definición de unión, $a \in X \cup Y$ o $a \in Z$ y por tanto, $a \in X$ o $a \in Y$ o $a \in Z$. Así, $a \in X$ o $a \in Y \cup Z$ lo que implica que $a \in X \cup (Y \cup Z)$. El otro contenido es idéntico.

Nota: Es posible que estas dos primeras demostraciones, de fáciles, sean confusas. Demostremos algo un poco menos evidente.

(vi). Demostremos una de las leyes Morgan: Sean $X, Y \subset T$, entonces

$$\overline{(X \cup Y)} = \overline{X} \cap \overline{Y}.$$

Como en los casos anteriores tendremos que demostrar el doble contenido:

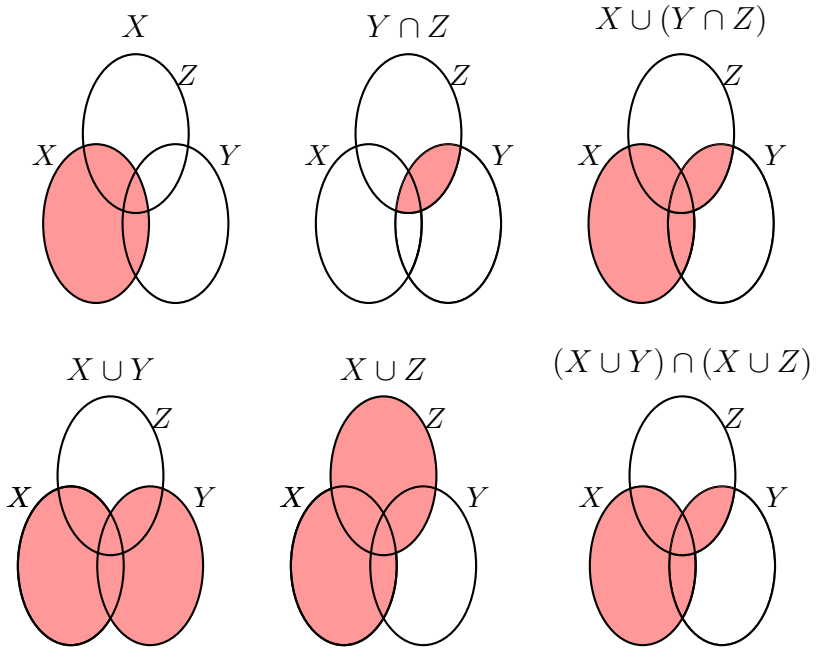
Sea $a \in \overline{(X \cup Y)}$. Por definición, a es un elemento de T que no es elemento de $X \cap Y$. Por tanto es un elemento de T que no es elemento de X ni elemento de Y. Como a no es elemento de X, $a \in \overline{X}$ y como a no es elemento de Y, $a \in \overline{Y}$. Por tanto $a \in \overline{X} \cap \overline{Y}$. Es decir,

$$\overline{(X \cup Y)} \subset \overline{X} \cap \overline{Y}.$$

Sea $a \in \overline{X} \cap \overline{Y}$. Tenemos entonces que por definición de intersección, $a \in \overline{X}$ y $a \in \overline{Y}$ o lo que es lo mismo, $a \notin X$ y $a \notin Y$. Por lo tanto, $a \notin X \cup Y$ o lo que es lo mismo, $a \in \overline{(X \cup Y)}$. Lo que nos demuestra el otro contenido,

$$\overline{X} \cap \overline{Y} \subset \overline{(X \cup Y)}.$$

Veamos un ejemplo de demostración por diagramas de Venn: (iii). $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ Representamos por diagramas de Ven los tres conjuntos X, Y, Z:



Luego $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$. El resto de la demostración no tiene mayor dificultad. ■

1.3. Conjuntos indexados

Normalmente tendremos que trabajar con más de dos conjuntos, posiblemente con una colección infinita, por tanto vamos a introducir la siguiente notación:

Definición 10 Cuando tengamos una familia de conjuntos, los nombraremos por letras (mayúsculas) con subíndices (**indexar**). Así, diremos: dada una familia de conjuntos X_i, con $i \in I$, (en donde I es un conjunto, llamado el conjunto de índices) lo que querrá decir que para cada elemento $i \in I$ tendremos el conjunto X_i.

Ejemplos E Consideremos para cada natural n los conjuntos

$$\begin{aligned} X_n : &= \{x \in \mathbb{N} \mid x \leq n\} \\ Y_n : &= \{x \in \mathbb{N} \mid x \geq n\}. \end{aligned}$$

Tenemos entonces que $X_7 = \{1, 2, 3, 4, 5, 6, 7\}$ o $X_{11} = \{1, 2, 3, \ldots, 10, 11\}$. Mientras que $Y_7 = \{7, 8, 9, \ldots\}$ e $Y_{1000} = \{1000, 1001, 1002, \ldots\}$.

Definición 11 Dada una familia de conjuntos X_i, con $i \in I$ (conjunto de índices). Se define la **unión** de los X_i y se representa por $\bigcup_{i\in I} X_i$ a un nuevo conjunto que tiene por elementos los elementos que pertenecen a algún X_i. Es decir:

$$\bigcup_{i\in I} X_i = \{z \mid \exists^{\S} i \text{ con } \ z \in X_i\}$$

Definición 12 Dada una familia de conjuntos X_i, con $i \in I$. Se define la **intersección** de los X_i y se representa por $\bigcap_{i\in I} X_i$ a un nuevo conjunto que tiene los elementos que están en todos los X_i.

$$\bigcap_{i\in I} X_i = \{z \mid \forall^{\P} i, \ z \in X_i\}$$

Definición 13 Dada una familia finita de conjuntos no vacíos X_i, con $i = \{1, 2, \ldots, n\}$ se define el **producto cartesiano** de los X_i y se representa por $X_1 \times X_2 \times \cdots \times X_n$ a un nuevo conjunto que tiene por elementos a todas las n-uplas $(x_1, x_2, \ldots, x_n)$ en donde cada $x_i \in X_i$ para $i \in \{1, 2, \ldots, n\}$.

$$X_1 \times X_2 \times \cdots \times X_n := \{(x_1, x_2, \ldots, x_n) \mid x_i \in X_i \text{ para } i = 1, 2, \ldots, n\}$$

Ejemplos F Dados $A = \{1, 2, a\}$, $B = \{a, b, c\}$ y $D = \{\alpha, \beta\}$,

$$\begin{aligned} A \times B \times C \ = \ & \{(1, a, \alpha), (1, b, \alpha), (1, c, \alpha), (2, a, \alpha), (2, b, \alpha), (2, c, \alpha), \\ & (a, a, \alpha), (a, b, \alpha), (a, c, \beta), (1, a, \beta), (1, b, \beta), (1, c, \beta), \\ & (2, a, \beta), (2, b, \beta), (2, c, \beta), (a, a, \beta), (a, b, \beta), (a, c, \beta)\} \end{aligned}$$

★ Los ejercicios del 1 al 5 de este tema pueden servirte para comprobar si has asimilado las nociones de esta sección.

[§] $\exists$: existe.

[¶] $\forall$: para todo.

2. Aplicaciones

2.1. Definiciones básicas

Definición 1 Sean X e Y dos conjuntos no vacíos. Se define una **correspondencia** de X en Y, como un subconjunto $C \subset X \times Y$.

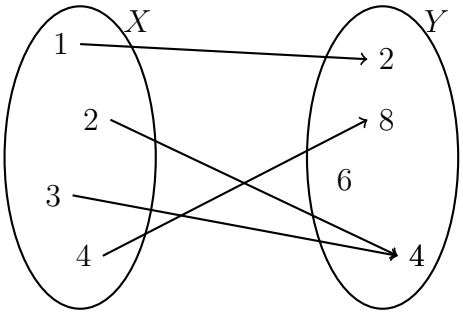
Siempre tienen problemas con la noción de aplicación.

Definición 2 Sean X e Y dos conjuntos no vacíos. Se define una **aplicación** f de X en Y, y se representa por $f : X \to Y$, como una correspondencia $F \subset X \times Y$ tal que para todo $x \in X$ existe un único $y \in Y$ con $(x, y) \in F$

$$\forall x \in X \quad \exists!\ y \in Y \quad | \quad (x, y) \in F^{\|}$$

Este elemento y no es más que lo que usualmente llamamos $f(x)$. Al conjunto X se le denomina el **dominio** de f y se representa por $\mathrm{Dom}(f)$. Al conjunto Y se le denomina el **codominio** de f y se representa por $\mathrm{CoDom}(f)$.

Ejemplos A Normalmente daremos una aplicación dando una regla que asigna a cada elemento de X un y sólo un elemento de Y. Podemos representar aplicaciones a partir de diagramas de Venn:



En este caso la aplicación f tiene dominio $X = \{1, 2, 3, 4\}$, codominio $Y = \{2, 4, 6, 8\}$ y consiste en el subconjunto $F = \{(1, 2), (2, 4), (3, 4), (4, 8)\} \subset X \times Y$. En este caso, f puede quedar representada por $f : X \to Y$ definida por $f(x) = -8 + 16x - 7x^2 + x^3$

Ejemplos B

$\star$ Sea $f : \mathbb{N} \to \mathbb{N}$ definida por $f(n) = 2n + 1$. En este caso la aplicación es el subconjunto $\{(n, 2n + 1) \mid n \in \mathbb{N}\}$.

$\star$ Sean X e Y dos conjuntos no vacíos y y_0 un elemento de Y. La **aplicación constante**: $f_{y_0} : X \to Y$ definida por $f(x) = y_0$ para todo $x \in X$. En este caso la aplicación es el subconjunto $\{(x, y_0) \mid x \in X\}$.

$\star$ La **aplicación identidad**: $\mathrm{Id}_X : X \to X$ definida por $\mathrm{Id}_X(x) = x$ para todo $x \in X$. En este caso la aplicación es el subconjunto $\{(x, x) \mid x \in X\}$.

$^{\|}\forall$ para todo; $\exists$ existe; ! un único; | tal que. En conjunto esta formula centrada se lee: para todo x perteneciente a X existe un único y perteneciente a Y tal que (x, y) pertenece a F

Definición 3 Diremos que dos aplicaciones f, g son **iguales** si $\mathrm{Dom}(f) = \mathrm{Dom}(g)$, $\mathrm{CoDom}(f) = \mathrm{CoDom}(g)$ y para todo $x \in \mathrm{Dom}(f)$ se tienen que $f(x) = g(x)$ (es decir, el subconjunto que las define es el mismo).

En el ejemplo A (Pag. 7) la aplicación f puede ser representada por

$$f : X \to Y \quad \text{con} \quad \begin{cases} f(x) = -8 + 16x - 7x^2 + x^3, \\ f(x) = 16 - 34x + 28x^2 - 9x^3 + x^4, \end{cases} \quad \text{o}$$

Ya que ambas definiciones de f tienen el mismo dominio, el mismo codominio y verifican que $f(1) = 2$, $f(2) = f(3) = 4$, y $f(4) = 8$, por lo que son la misma aplicación.

Fin de clase 2; 29-09-2011, grupo A y B

Otra vez nos encontramos aquí con un concepto nuevo (son dos imagen e imagen inversa). Explicar el concepto ¿con diagramas de Venn? y luego dar la definición matemática.

Definición 4 Sean X e Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación.

• Dado un subconjunto A de X se define la imagen de A por f y se denota por $f(A)$ como:

$$f(A) := \{f(a) \mid a \in A\} \subset Y$$

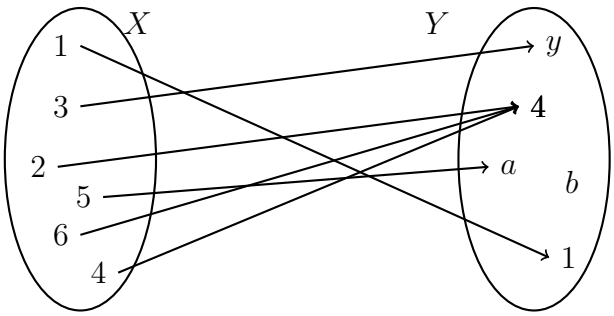
Se define la **imagen** de f como $\mathrm{Im}(f) := f(X)$.

Nota: Visto en diagramas de Venn, la imagen de f son los elementos de Y a los que les llega alguna flecha de algún elemento de X. Si miramos la aplicación dada en el ejemplo C (Pag. 8) (un párrafo abajo) la aplicación f tiene por imagen $\mathrm{Im}(f) := \{y, 4, a, 1\}$.

• Dado un subconjunto B de Y se define la **imagen inversa** de B por f y se denota por $f^{-1}(B)$ como:

$$f^{-1}(B) := \{x \in X \mid f(x) \in B\} \subset X$$

Ejemplos C *Consideremos la aplicación:*



Tenemos entonces que

$$f(\{1,2,3\}) = \{1,4,y\}, \quad f(\{2,4,6\}) = \{4\}, \quad f(\{4,5\}) = \{4,a\}$$
$$f^{-1}(\{b\}) = \emptyset, \quad f^{-1}(\{4\}) = \{2,4,6\}, \quad f^{-1}(\{a,4,y\}) = \{2,3,4,5,6\}$$

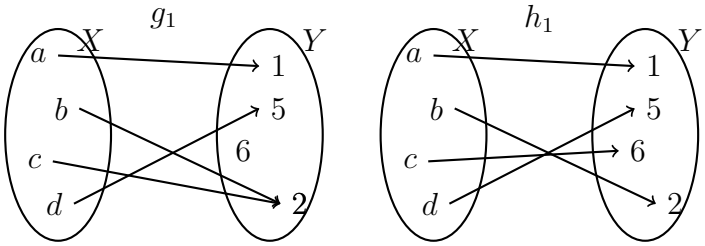
Nota: Dada una aplicación $f : X \to Y$ acabamos de definir dos aplicaciones:

$$\Phi_f : \mathcal{P}(X) \to \mathcal{P}(Y) \text{ definida por } \Phi_f(A) := f(A)$$
$$\Psi_f : \mathcal{P}(Y) \to \mathcal{P}(X) \text{ definida por } \Psi_f(B) := f^{-1}(B)$$

Siempre tienen problemas con inyectiva, sobreyectiva, biyectiva. Hay que dar la noción intuitiva (diagramas de Venn), la definición matemática y en la practica como se demuestra que una aplicación es...

Definición 5 Sean X e Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación. Diremos que f es:

• **inyectiva**: Si para todo par de elementos $x, y \in X$, con $x \neq y$, se tiene que $f(x) \neq f(y)$. Es decir, dos elementos distintos de X no pueden ir a para al mismo sitio. Esta noción es bastante clara cuando usamos diagramas de Venn:



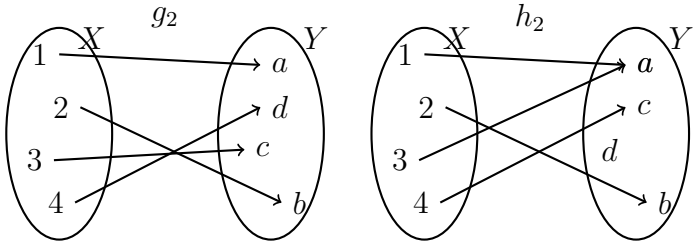
La aplicación g_1 no es inyectiva, ya que al elemento 2 de Y le llegan dos flechas (b y c son dos elementos distintos de X que tienen por imagen el 2. La aplicación h_1 si es inyectiva, a ningún elemento de Y le llegan dos flechas).

Nota: la inyectividad significa que dos elementos distintos van a parar a sitios distintos, o lo que es lo mismo, que un elemento de Y no puede ser imagen de dos elementos de X. Por tanto, para demostrar que una aplicación f es inyectiva se supondrá que hay "dos" elementos $x, x' \in X$ tales que $f(x) = f(x')$ y se demostrará que $x = x'$. Estamos usando la equivalencia de los enunciados:

$$\text{si p entonces q} \quad \Longleftrightarrow \quad \text{si no q entonces no p}$$

en donde p es "x es distinto de x'" , q es "$f(x)$ es distinto de $f(x')$" y por tanto, no p es x es igual a x' y no q es $f(x)$ es igual que $f(x')$.

• **sobreyectiva**: si para todo $y \in Y$ existe un $x \in X$ tal que $f(x) = y$. Es decir, todo elemento de Y es imagen de algún elemento de X. Al igual que con la noción de inyectividad, la sobreyectividad es bastante clara usando diagramas de Venn:



La aplicación g_2 es sobreyectiva, ya que a todo elemento de Y le llega una flecha. La aplicación h_2 no es sobreyectiva, ya que d no es imagen de ningún elemento de X (a d no le llega ninguna flecha).

• **biyectiva**: si es a la vez inyectiva y sobreyectiva. Las aplicaciones h_1 y g_2 son biyectivas, ya que a cada elemento de Y le llega una y sólo una flecha de X.

Ejemplos D

⋆ Dada una aplicación $f : X \to Y$ y dado X' un subconjunto de X tenemos la **restricción de** f a X' como: $f|_{X'} : X' \to Y$ definida por $f|_{X'}(x) = f(x)$.

⋆ Dada una aplicación $f : X \to Y$ y dado Y' un subconjunto de Y con $\mathrm{Im}(f) \subset Y'$ tenemos **restricción de** f a Y' como: $f|_{Y'} : X \to Y'$ definida por $f|_{Y'}(x) = f(x)$.

Lema 6 Sean X e Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación. Entonces:

(i) f es sobreyectiva si y sólo si $\mathrm{Im}(f) = Y$.

(ii) La restricción de una aplicación f a su imagen, $f|_{\mathrm{Im}(f)} : X \to \mathrm{Im}(f)$ es una aplicación sobreyectiva.

(iii) Si $f : X \to Y$ es inyectiva y X' es un subconjunto de X, entonces $f|_{X'} : X' \to Y$ es también inyectiva.

(iv) $f : X \to Y$ es inyectiva si y sólo si para todo $y \in Y$ el conjunto $f^{-1}(\{y\})$ tiene como mucho un elementos. (ejercicio)

(v) $f : X \to Y$ es sobreyectiva si y sólo si para todo $y \in Y$ el conjunto $f^{-1}(\{y\})$ tiene al menos un elemento. (ejercicio)

Demo: Los tres apartados son obvios (tenéis que demostrarlo vosotros). ■

Ejemplos E

⋆ La aplicación $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = 2x + 1$ es biyectiva.

⋆ La aplicación $g : \mathbb{N} \to \mathbb{N}$ definida por $g(x) = 2x + 1$ es sólo inyectiva. No existe ningún natural n tal que $f(n) = 4$.

⋆ La aplicación $h : \mathbb{R} \to \mathbb{R}$ definida por $h(x) = x^2$ no es ni inyectiva ni sobreyectiva. $h(2) = h(-2)$ por lo que no es inyectiva y no existe ningún elemento $x \in \mathbb{R}$ tal que $f(x) = -1$, por lo que no es sobreyectiva.

2.2. Composición de aplicaciones

Definición 7 Sean X, Y, Z tres conjuntos y $f : X \to Y$ y $g : Y \to Z$ dos aplicaciones. Se define la **composición** de f con g y se representa por $g \circ f$ como la aplicación

$$g \circ f : X \to Z \quad \text{definida por } g \circ f(x) := g(f(x)) \quad \forall\, x \in X$$

Nota: Observar que el dominio de $g \circ f$ es el dominio de f y el recorrido de $g \circ f$ es el recorrido de g.

Ejemplos F *Sea $\mathbb{N}$ el conjunto de los naturales y sean $f : \mathbb{N} \to \mathbb{N}$ y $g : \mathbb{N} \to \mathbb{N}$ las aplicaciones definidas por:*

$$f(n) = 2n + 1 \quad y \quad g(n) = n^2$$

Tenemos entonces que $g \circ f$ es la aplicación $g \circ f : \mathbb{N} \to \mathbb{N}$ definida por

$$g \circ f(n) = g(f(n)) = g(2n + 1) = (2n + 1)^2.$$

Y que $f \circ g$ es la aplicación $f \circ g : \mathbb{N} \to \mathbb{N}$ definida por

$$f \circ g(n) = f(g(n)) = g(n^2) = 2n^2 + 1.$$

Teorema 8 Sean X, Y, Z y T cuatro conjuntos no vacíos y consideremos

$$f : X \to Y, \quad g : Y \to Z, \quad h : Z \to T$$

tres aplicaciones. Entonces $h \circ (g \circ f) = (h \circ g) \circ f$.

Demo: Es una mera comprobación: El dominio de ambas aplicaciones es X y el codominio de ambas aplicaciones es T. Es más, dado cualquier $x \in X$ se tiene que,

$$h \circ (g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x)))$$
$$(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x)))$$

Luego las aplicaciones $h \circ (g \circ f)$ y $(h \circ g) \circ f$ coinciden para todo $x \in X$, lo que demuestra que son la misma aplicación, ver definición 3 (Pag. 8). ■

Nota: La composición de aplicaciones no tiene que verificar la propiedad conmutativa. Es más, si dominio y codominio no son el mismo conjunto no tiene sentido esta pregunta, e incluso si X un conjunto no vacío y $f, g : X \to X$ son dos aplicaciones no tiene que verificarse que $f \circ g = g \circ f$.

Ver definición de Id_X en el ejemplo B$\star_3$ (Pag. 7).

Lema 9 Sean X e Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación.

(i) Si Id_Y denotan la aplicación identidad en Y, entonces $\mathrm{Id}_Y \circ f = f$.

(ii) Si Id_X denotan la aplicación identidad en X, entonces $f \circ \mathrm{Id}_X = f$.

Demo: Los dos apartados son obvios. ■

Proposición 10 Sean X, Y y Z tres conjuntos no vacíos y $f : X \to Y$, $g : Y \to Z$ dos aplicaciones. Entonces:

(i) Si f y g son inyectivas, entonces $g \circ f$ es inyectiva.

(ii) Si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva. (ejercicio)

(iii) Si $g \circ f$ es inyectiva, entonces f es inyectiva. (ejercicio)

(iv) Si $g \circ f$ es sobreyectiva, entonces g es sobreyectiva.

(v) f y g son biyectivas, entonces $g \circ f$ es biyectiva.

Demo:

(i). Supongamos que f y g son dos aplicaciones inyectivas y consideremos $x_1, x_2 \in X$ tales que $g \circ f(x_1) = g \circ f(x_2)$ (tenemos que demostrar, para ver que $g \circ f$ es inyectiva, que $x_1 = x_2$). Por definición

$$g(f(x_1)) = g \circ f(x_1) = g \circ f(x_2) = g(f(x_2))$$

por tanto, como g es inyectiva, $f(x_1) = f(x_2)$ y como f es inyectiva $x_1 = x_2$.

(iv). Supongamos que $g \circ f : X \to Z$ es una aplicación sobreyectiva y veamos que $g : Y \to Z$ es también sobreyectiva. Dado $z \in Z$ tenemos que encontrar un $y \in Y$ tal que $g(y) = z$. Como $g \circ f$ es sobreyectiva, existe $x \in X$ tal que $z = g \circ f(x) = g(f(x))$. Por tanto, $y = f(x)$ es el elemento que buscamos:

$$g(y) = g(f(x)) = g \circ f(x) = z$$

(v) es corolario de (i) y (ii). ■

Es claro que estos resultados les cuesta.

Fin de clase 3; 30-09-2011, grupo A y B

Proposición 11 Sean X e Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación. Entonces,

(i) f es sobreyectiva si y sólo si existe $g : Y \to X$ tal que $f \circ g = Id_Y$. Es más, si g es única, f es biyectiva.

(ii) f es inyectiva si y sólo si existe $g : Y \to X$ tal que $g \circ f = \mathrm{Id}_X$. Es más, si g es única, f es biyectiva o $\#X = 1$ **.

Demo: (i) Si existe una aplicación $g : Y \to X$ tal que $f \circ g = \mathrm{Id}_Y$, por la proposición 10(iv) (Pag. 11), f es sobreyectiva (ya que la aplicación Id_Y es sobreyectiva). Supongamos ahora que $f : X \to Y$ es una aplicación sobreyectiva (para terminar de demostrar el apartado tenemos que construir una aplicación $g : Y \to X$ tal que $f \circ g = \mathrm{Id}_Y$). Dado $y \in Y$ como f es sobreyectiva, $f^{-1}(\{y\}) \neq \emptyset$. Por tanto para cada $y \in Y$ elegimos un $x \in f^{-1}(\{y\})$ y definimos $g : Y \to X$ como

$$g(y) = x \quad \text{siendo } x \text{ el elemento elegido anteriormente en } f^{-1}(\{y\}).$$

Tenemos entonces que $f \circ g(y) = f(g(y)) = y$ (ya que por construcción $g(y) \in f^{-1}(\{y\})$. Es más como la elección de $x \in f^{-1}(\{y\})$ es arbitraria, si existe un $y \in Y$ tal que el conjunto $f^{-1}(\{y\})$ tiene más de un elemento, entonces podemos definir más de una g, en caso contrario, si para todo $y \in Y$ el conjunto $f^{-1}(\{y\})$ tiene un elemento, la aplicación es inyectiva, ver el ejercicio 12 (Pag. 25).

**ver la definición 3 (Pag. 22)

(ii) Si existe una aplicación $g : Y \to X$ tal que $g \circ f = \mathrm{Id}_X$, por la proposición 10(iii) (Pag. 11), f es inyectiva (ya que la aplicación Id_X es inyectiva). Supongamos ahora que $f : X \to Y$ es una aplicación inyectiva (para terminar de demostrar el apartado tenemos que construir una aplicación $g : Y \to X$ tal que $g \circ f = \mathrm{Id}_X$). Sea $\mathrm{Im}(f)$ la imagen de f y consideremos $Y = \mathrm{Im}(f) \cup \overline{\mathrm{Im}(f)}$ (Y queda partido en dos trozos, por un lado la imagen de f y por el otro lo que falta, el complemento de la imagen). Por último elegimos un elemento arbitrario de X, llamándolo x_0. Definimos entonces la aplicación g. Dado $y \in Y$:

$$g(y) := \begin{cases} x, & \text{si } y \in \mathrm{Im}(f) \text{ donde x es el único elemento de } X \text{ tal que } f(x) = y; \\ x_0, & \text{si } y \notin \mathrm{Im}(f). \end{cases}$$

Tenemos entonces que $g \circ f(x) = g(f(x))$ y por como hemos definido g, como $f(x) \in \mathrm{Im}(f)$, $g(f(x))$ es el único elemento de X, llamémoslo a, tal que $f(a) = f(x)$ es decir, $g(f(x)) = x$. Por último, observar que si $\#X > 1$ y f no es sobreyectiva, es decir, $\mathrm{Im}(f) \neq Y$ (o equivalentemente $\overline{\mathrm{Im}(f)} \neq \emptyset$) podemos definir más de una g (cada vez que cambiamos el x_0 [por hipótesis hay más de uno] tenemos una nueva g que verifica la tesis). ■

Teorema 12 Sean X e Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación. Las siguientes condiciones son equivalentes:

(i) f es biyectiva.

(ii) Existe una aplicación $g : Y \to X$ tal que $f \circ g = \mathrm{Id}_Y$ y $g \circ f = \mathrm{Id}_X$.

Es más, g es única, que denotaremos por f^{-1}. En este caso se dice que f es **inversible** con inversa f^{-1}.

Demo: Supongamos que estamos en las condiciones de (ii). Entonces por la proposición 11(i) (Pag. 12) f es sobreyectiva, ya que $f \circ g = \mathrm{Id}_Y$ y por la proposición 11(ii) (Pag. 12) f es inyectiva, ya que $g \circ f = \mathrm{Id}_X$. Por tanto f es biyectiva. Supongamos ahora que f es biyectiva. Entonces, como f es sobreyectiva, por la proposición 11(i) (Pag. 12) existe una aplicación $g : Y \to X$ tal que $f \circ g = \mathrm{Id}_Y$ y como f es inyectiva, por la proposición 11(ii) (Pag. 12) existe una aplicación $g' : Y \to X$ tal que $g' \circ f = \mathrm{Id}_X$ (nadie nos asegura en principio que tengan que ser la misma). Por último,

$$g' = g' \circ \mathrm{Id}_Y = g' \circ (f \circ g) = (g' \circ f) \circ g = \mathrm{Id}_X \circ g = g$$

Es más, la identidad anterior nos demuestra que g es única. ■

Proposición 13 Sean X, Y y Z tres conjuntos no vacíos y $f : X \to Y$ y $g : Y \to Z$ dos aplicaciones biyectivas. Entonces $g \circ f$ es biyectiva, por tanto inversible con inversa,

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Demo: Comprobemos simplemente que $f^{-1} \circ g^{-1}$ es la inversa de $g \circ f$. Tendremos entonces que $g \circ f$ es biyectiva por el Teorema 12 (Pag. 13).

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{Id}_Y \circ f = f^{-1} \circ f = \mathrm{Id}_X$$
$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{Id}_X \circ g^{-1} = g \circ g^{-1} = \mathrm{Id}_Y .$$

Lo que demuestra la proposición. ■

Nota: Dados dos conjuntos no vacíos X, Y y una aplicación $f : X \to Y$ NO SE DEBE CONFUNDIR la imagen inversa de un subconjunto B de Y por f, denotado por $f^{-1}(B)$, con la inversa de la aplicación (QUE SÓLO EXISTIRÁ SI f ES BIYECTIVA).

★ Los ejercicios del 7 al 18 de este tema pueden servirte para comprobar si has asimilado las nociones de esta sección.

Fin de clase 4; 04-10-2011, grupo A y B

3. Relaciones

Definición 1 Se define una **relación** en un conjunto no vacío X, y se denota por $\mathcal{R}$, como cualquier subconjunto del producto cartesiano $X \times X$. Si un elemento $(a, b) \in \mathcal{R}$ diremos que a está relacionado con b y lo denotaremos por $a \mathcal{R} b$.

Ejemplos A

⋆ En el conjunto de los números naturales definimos la relación "ser menor o igual que", es decir, diremos $n \mathcal{R} m$ si y sólo si $n \leq m$. Así, $3 \mathcal{R} 5$ si están relacionados, mientras que $5 \mathcal{R} 2$ no.

⋆ Podemos considerar, en el conjunto de los seres humanos, la relación "ser hermano de".

Definición 2 Sea X un conjunto no vacío y $\mathcal{R}$ una relación en X. Diremos que $\mathcal{R}$ verifica la propiedad:

- **Reflexiva:** Para todo $x \in X$, se tiene que $x \mathcal{R} x$.
- **Transitiva:** Si $x \mathcal{R} y$ e $y \mathcal{R} z$, entonces $x \mathcal{R} z$.
- **Simétrica:** Si $x \mathcal{R} y$, entonces $y \mathcal{R} x$.
- **Antisimétrica:** Si $x \mathcal{R} y$ e $y \mathcal{R} x$, entonces $x = y$.

La antisimétrica se puede enunciar si $x \mathcal{R} y$ y $x \neq y$ entonces y no esta relacionado con x.

Ejemplos B *Consideremos las siguientes relaciones:*

$$\begin{aligned}
\mathcal{R} &:= \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \textit{ divide a } y\} \\
\mathcal{R}' &:= \{(x, x+1) \mid \textit{ con } x \in \mathbb{N}\} \\
\mathcal{R}'' &:= \{(1,1), (2,2), (a,a), (1,a), (a,1)\} \textit{ en } A = \{1, 2, a\}
\end{aligned}$$

Entonces: $\mathcal{R}$ es reflexiva, transitiva y antisimétrica (no es simétrica). $\mathcal{R}'$ verifica solamente la propiedad antisimétrica. $\mathcal{R}''$ es reflexiva, transitiva y simétrica (no es antisimétrica).

3.1. Relación de equivalencia.

Definición 3 Sea X un conjunto no vacío y $\mathcal{R}$ una relación en X. Diremos que $\mathcal{R}$ es una **relación de equivalencia** si verifica las propiedades reflexiva, transitiva y simétrica.

Ejemplos C (La relación de Congruencia) Sea $\mathbb{Z}$ el conjunto de los enteros y sea $n \in \mathbb{Z}$. Definimos la relación

$$a\mathcal{R}b \quad \Longleftrightarrow \quad a - b = \dot{n} \quad (a - b \text{ es multiplo de } n)$$

Tenemos que $\mathcal{R}$ es una relación de equivalencia, llamada la **relación de congruencia modulo** n. Esta relación se denota de forma especial. Así, si dos enteros $a, b \in \mathbb{Z}$ están relacionados se denotará por $a \equiv b \pmod{n}$.

Demo: Veamos que la relación de congruencia verifica las propiedades reflexiva, transitiva y simétrica:

(i). Reflexiva: dado $x \in \mathbb{Z}$, tenemos que $x - x = 0 \cdot n$ por lo que $x \equiv x (\mathrm{mod}\, n)$.

(ii). Transitiva: Sean $x, y, z \in \mathbb{Z}$ tales que $x \equiv y \pmod{n}$ e $y \equiv z \pmod{n}$. Tenemos entonces que existe un $\alpha \in \mathbb{Z}$ tal que $x - y = \alpha n$ y existe un $\beta \in \mathbb{Z}$ tal que $y - z = \beta n$. Por tanto

$$x - z = (x - y) + (y - z) = \alpha n + \beta n = (\alpha + \beta)n.$$

Luego $x \equiv z (\mathrm{mod}\, n)$.

(iii). Simétrica: Sean $x, y \in \mathbb{N}$ tales que $x \equiv y (\mathrm{mod}\, n)$. Por definición existe $\alpha \in \mathbb{Z}$ tal que $x - y = \alpha n$. Así, $y - x = (-\alpha)n$ y por tanto $y \equiv x (\mathrm{mod}\, n)$. ■

Ejemplos D *Sean X, Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación. Entonces la relación $a\mathcal{R}b \iff f(a) = f(b)$ es de equivalencia.* *(Ejercicio)*

La siguiente definición nos va a permitir construir nuevos ejemplos de relaciones de equivalencia. Como veremos al final de esta sección, cualquier relación de equivalencia será de este tipo.

Definición 4 Sea X un conjunto no vacío y $\mathcal{P} = \{A_i\}_{i \in I}$ una familia de subconjuntos de X. Diremos que $\mathcal{P}$ es una **partición** de X si:

- Para todo $i \in I$, se tiene que $A_i \neq \emptyset$.
- Dados $i, j \in I$, con $i \neq j$, se tiene que $A_i \cap A_j = \emptyset$.
- $\bigcup_{i \in I} A_i = X$.

Teorema 5 Sea X un conjunto no vació y sea $\mathcal{P} = \{A_i\}_{i \in I}$ una partición en X. Entonces la relación $x\mathcal{R}y$ si y sólo si x, y están en un mismo trozo de la partición, es decir,

$$x\mathcal{R}y \quad \Longleftrightarrow \quad \exists\, i \in I \mid x, y \in A_i,$$

es una relación de equivalencia en X.

Demo: Veamos que $\mathcal{R}$ verifica las propiedades reflexiva, transitiva y simétrica:

(i). Reflexiva: dado $x \in X$, por la propiedad tercera de la definición de partición se tiene que $x \in X = \cup_{i\in I} A_i$ por tanto existe un $i \in I$ tal que $x \in A_i$ y así, $x\mathcal{R}x$.

(ii). Transitiva: Sean $x, y, z \in X$ tal que $x\mathcal{R}y$ e $y\mathcal{R}z$. Por definición, existe $i \in I$ tal que $x, y \in A_i$ y existe un $j \in I$ tal que $y, z \in A_j$. Por tanto $y \in A_i \cap A_j$ y por la propiedad segunda de la definición de partición $i = j$. Así, $x, y, z \in A_i (= A_j)$, y por tanto $x\mathcal{R}z$.

(iii). Simétrica: Sean $x, y \in X$ tales que $x\mathcal{R}y$. Por definición existe $i_0 \in I$ tal que $x, y \in A_{i_0}$ y por tanto $y\mathcal{R}x$. ■

Ejemplos E *Sea X un conjunto no vacío y $\mathcal{P}$ una partición en X. Entonces, el teorema anterior nos permite asociar una relación de equivalencia a la partición $\mathcal{P}$ que se denotará por $\mathcal{R}_{\mathcal{P}}$.*

Desde este momento, hasta el final de la sección vamos a demostrar que toda relación de equivalencia es de este tipo. Es decir, si tenemos una relación de equivalencia $\mathcal{R}$ en un conjunto no vacío X podemos construir una partición $\mathcal{P}$ en X tal que $\mathcal{R}$ es exactamente la relación de equivalencia asociada a $\mathcal{P}$.

Definición 6 Sea X un conjunto no vacío y $\mathcal{R}$ una relación de equivalencia en X. Dado un elemento $x \in X$ definimos la **clase de equivalencia** de x y la representamos por $[x]$ o $\overline{x}$ como el conjunto:

$$\overline{x} = \{y \in X \mid x \,\mathcal{R}\, y\} \subset X$$

Nota: Observar que la propiedad reflexiva nos asegura que $x \in \overline{x}$.

El conjunto de todas las clases de equivalencia de una relación $\mathcal{R}$ en un conjunto X se le llamará el **conjunto cociente** de X respecto de $\mathcal{R}$ y se denotará por $X/\,\mathcal{R}$ o $X/_{\approx}$

Ejemplos F $\star$ Consideremos la relación de congruencia mod 3. Tenemos entonces que

$$\begin{aligned}
\overline{0} &= \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 3\} = \{3x \quad\; x \in \mathbb{Z}\} = \{\cdots, -6, -3, 0, 3, 6, \cdots\} \\
\overline{1} &= \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 3\} = \{3x+1 \quad x \in \mathbb{Z}\} = \{\cdots, -5, -2, 1, 4, 7, \cdots\} \\
\overline{2} &= \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 3\} = \{3x+2 \quad x \in \mathbb{Z}\} = \{\cdots, -4, -1, 2, 5, 8, \cdots\}
\end{aligned}$$

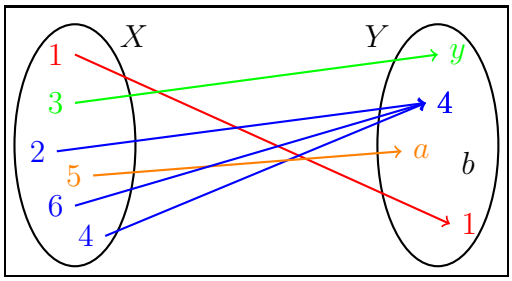
Observar que $\overline{0} = \overline{3} = \overline{6}$ =etc y que los subconjuntos $\{\overline{0}, \overline{1}, \overline{2}\}$ son una partición de $\mathbb{Z}$.

$\star$ Sea $A = \{1, 2, a\}$ y $\mathcal{R}$= $\{(1,1), (2,2), (a,a), (1,a), (a,1)\}$. Entonces $\mathcal{R}$ es una relación de equivalencia y $A/_{\approx} = \{\{1, a\}, \{2\}\}$ (observar que forman una partición de X).

$\star$ Sean X, Y dos conjuntos no vacíos, $f : X \to Y$ una aplicación y consideremos la relación de equivalencia en X: $a\mathcal{R}b \iff f(a) = f(b)$. Entonces, para todo $a \in X$,

$$\overline{a} = \{x \in X \mid f(x) = f(a)\} = f^{-1}(f(a))$$

Aunque pueda ser aquí un poco más difícil de visualizar, nos encontramos otra vez con que el conjunto cociente es un realidad una partición de X. Por ejemplo, si consideramos la aplicación dada en el ejemplo C (Pag. 8),



Tenemos que el conjunto cociente respecto de esta relación es $X/_{\approx} = \{\{1\}, \{2,4,6\}, \{3\}, \{5\}\}$. Observar que, en este caso también, se trata de una partición del conjunto X.

Teorema 7 Sea X un conjunto no vacío y sea $\mathcal{R}$ una relación de equivalencia en X. Entonces la familia de las clases de equivalencia de elementos de X es una partición de X, denotada por $\mathcal{P}_{\mathcal{R}}$. Es más,

(i) Para todo $x \in X$ se tiene que $x \in \overline{x}$.

(ii) $x\mathcal{R}y$ si y sólo si $x \in \overline{y}$ ($\iff$ $y \in \overline{x}$).

(iii) $x\mathcal{R}y$ si y sólo si $\overline{x} = \overline{y}$.

(iv) $x\mathcal{R}y$ si y sólo si existe $z \in X$ tal que $x, y \in \overline{z}$.

Observar que (iv) lo que dice es que la relación $\mathcal{R}$ es la relación de equivalencia asociada a la partición $\mathcal{P}_{\mathcal{R}}$.

Demo: Vamos a demostrar los cuatro apartados, ya que ellos nos demostraran el teorema.

(i). Por la propiedad reflexiva $x\mathcal{R}x$, por lo que por definición $x \in \overline{x} = \{y \in X \mid x\mathcal{R}y\}$.

(ii). Este apartado más bien es un recordatorio, ya que $x\mathcal{R}y$, si y sólo si $y \in \overline{x}$ (por simetría, $x \in \overline{y}$).

(iii). Supongamos que $x\mathcal{R}y$ y veamos que $\overline{x} = \overline{y}$. Veamos ambos contenidos: sea $z \in \overline{x}$, entonces $x\mathcal{R}z$. Por la propiedad simétrica, $z\mathcal{R}x$ y como tenemos $x\mathcal{R}y$, la propiedad transitiva nos demuestra que $z\mathcal{R}y$ es decir, $z \in \overline{y}$. De forma similar, si $z \in \overline{x}$ se tiene que $z \in \overline{y}$, por lo que $\overline{x} = \overline{y}$.

Supongamos ahora que $\overline{x} = \overline{y}$. Entonces, por (i), $x \in \overline{x} = \overline{y}$ y por tanto, ver (ii), $x\mathcal{R}y$.

(iv) Supongamos que $x\mathcal{R}y$, entonces, por (i) y (iii), $x, y \in \overline{x} = \overline{y}$. Supongamos ahora que existe un $z \in X$ tal que $x, y \in \overline{z}$. Entonces, $x\mathcal{R}z$ y $y\mathcal{R}z$. Por tanto, aplicando la propiedad simétrica, $x\mathcal{R}z$ y $z\mathcal{R}y$ y por la transitiva, $x\mathcal{R}y$.

Por último, para cada $x \in X$, $x \in \overline{x}$ por lo que $\overline{x} \neq \emptyset$. Por otro lado, si $\overline{x} \cap \overline{y} \neq \emptyset$, existe $z \in \overline{x} \cap \overline{y}$ y por tanto, por (ii), $z \cap Rx$ y $z \cap Ry$ por lo que por (iii), $\overline{x} = \overline{z} = \overline{y}$. Claramente se tiene que $\bigcup_{x \in X} \overline{x} = X$. Lo que demuestra que las clases de equivalencia de $\mathcal{R}$ definen una partición en X y (iv) demuestra que $\mathcal{R}$ es la relación asociada a esta partición. ■

Fin de clase 5; 06-10-2011, grupo A y B

Nota: Este teorema nos demuestra que los conceptos de partición y relación de equivalencia son el mismo. Es decir, si tenemos una relación de equivalencia la podemos ver como una partición y si tenemos una partición la podemos ver como una relación de equivalencia.

Nota: Observar que por el apartado 3 del teorema anterior si $x\mathcal{R}y$, $\overline{x} = \overline{y}$, es decir, que el subconjunto $\overline{x} \subset X$ también se puede representar por $\overline{y}$. Por tanto, un mismo elemento del conjunto cociente $X/_{\approx}$ se podrán nombrar usando distintos representantes. Por ejemplo, si consideramos la relación de congruencia modulo 3, tenemos que el conjunto cociente es

$$\mathbb{Z}/\bmod n = \{\overline{1}, \overline{2}, \overline{3}\} = \{\overline{10}, \overline{29}, \overline{99}\}$$

Ya que $1 \equiv 10 \pmod 3$ y por tanto $\overline{1} = \overline{10}$, $2 \equiv 29 (\mathrm{mod}\, 3)$ y por tanto $\overline{2} = \overline{29}$ y $3 \equiv 99 \pmod 3$ y por tanto $\overline{3} = \overline{99}$. Como veremos más adelante esta posibilidad de representar los elementos del conjunto cociente de distintas maneras nos obligara a ser muy precavidos cuando trabajemos con estos conjuntos.

Definición 8 Sea X un conjunto no vacío y $\mathcal{R}$ una relación de equivalencia en X. Recordamos que el conjunto cociente de X respecto de $\mathcal{R}$ es el conjunto de todas las clases de equivalencia de X (que acabamos de demostrar forman una partición de X. Este conjunto cociente lo denotamos por $X/\mathcal{R}$ o $X/_{\approx}$

Definición 9 Sea X un conjunto no vacío y $\mathcal{R}$ una relación de equivalencia en X. Se define la **aplicación canónica** de X en $X/_{\approx}$ como la aplicación $\pi : X \to X/_{\approx}$ definida por $\pi(x) = \overline{x}$.

Corolario 10 Sea X un conjunto no vacío y sea $\mathcal{R}$ una relación de equivalencia en X. Sea $X/\mathcal{R}$ el conjunto cociente y $\pi : X \to X/\mathcal{R}$ la proyección canónica al cociente. Entonces para todo $x, y \in X$ se tiene que

$$x\mathcal{R}y \iff \pi(x) = \pi(y)$$

Por lo que $\mathcal{R}$ también puede verse como la relación asociada a la aplicación canónica.

Demo: Es el apartado (iii) del teorema anterior. ■

Hemos demostrado que cualquier relación de equivalencia se puede ver como una partición y se puede ver como la relación de equivalencia asociada a una aplicación.

3.2. Relación de orden.

Definición 11 Sea X un conjunto no vacío y $\mathcal{R}$ una relación en X. Diremos que $\mathcal{R}$ es una **relación de orden** si verifica las propiedades reflexiva, transitiva y antisimétrica. Normalmente denotaremos las relaciones de orden por el signo $\leq$ y diremos que el par $(X, \leq)$ es un **conjunto ordenado**.

Ejemplos G

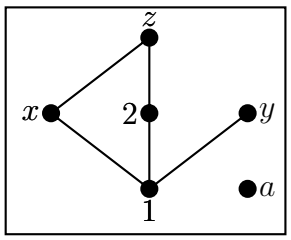
⋆ Considerar la relación de "mayor o igual" o "menor o igual" en $\mathbb{N}$, $\mathbb{Q}$ ó $\mathbb{R}$.

⋆ Sea X un conjunto. Entonces $(\mathcal{P}(X), \subseteq)$ es un conjunto ordenado.

⋆ Sea $A = \{1, 2, a, x, y, z\}$ entonces la relación siguiente es una relación de orden en A,

$$\mathcal{R}= \{(1,1), (2,2), (a,a), (x,x), (y,y), (z,z), (1,2), (1,x), (1,z), (2,z), (1,y), (x,z)\}.$$

Observación: Podemos representar las relaciones de orden usando **grafos**, en donde una linea entre dos elementos de distinta altura significa que están relacionados y el elemento de más altura es el mayor. Así, la relación de orden anterior queda representada por el grafo:
Observar: a no está relacionado con ningún otro elemento de A.



Definición 12 Sea $(X, \leq)$ un conjunto ordenado. Diremos que dos elementos $x, y \in X$ son **comparables** si $a \leq b$ o $b \leq a$. En caso contrario diremos que son **no comparables**.

Por ejemplo en la relación de orden dada en el ejemplo G ($\star_3$) (Pag. 18) se tiene que 2 y x no son comparable. Es más, el elemento b sólo es comparable consigo mismo.

Definición 13 Sea $(X, \leq)$ un conjunto ordenado. Diremos que $\leq$ es un **orden total** si dos elementos cualesquiera de X son comparables.

Definición 14 (Elementos Notables en un conjunto ordenado). Sea $(X, \leq)$ un conjunto ordenado y sea $Y \subset X$.

• Se define una **cota superior** o **mayorante** para Y como cualquier elemento $x \in X$ tal que para todo $y \in Y$, $y \leq x$.

$$x \in X \text{ es una cota superior} \iff \forall\, y \in Y, \quad y \leq x.$$

• Se define una **cota inferior** o **minorante** para Y como cualquier elemento $x \in X$ tal que para todo $y \in Y$, $x \leq y$.

$$x \in X \text{ es una cota inferior} \iff \forall\, y \in Y, \quad x \leq y.$$

• Se define el **supremo** para Y, y se denota por $\mathrm{Sup}(Y)$, como la menor de las cotas superiores.

$$x = \mathrm{Sup}(Y) \iff \quad x \text{ es cota superior y } \forall z \text{ cota superior } \; x \leq z.$$

Cuando el supremo pertenece a Y se le denomina **máximo** y se le denota por $\mathrm{Max}(Y)$

• Se define el **ínfimo** para Y, y se denota por $\mathrm{ínf}(Y)$, como la mayor de las cotas inferiores.

$$x = \mathrm{Inf}(Y) \iff \quad x \text{ es cota inferior y } \forall z \text{ cota inferior } \; z \leq x.$$

Cuando el ínfimo de Y pertenece a Y se le denomina **mínimo** y se le denota por $\mathrm{Min}(Y)$.

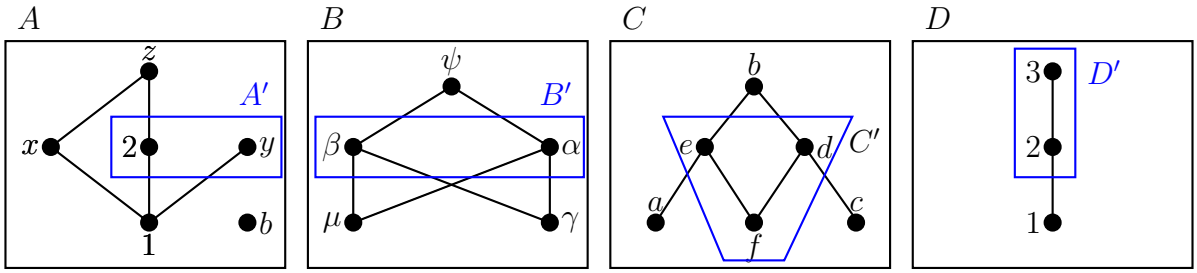
• Se dice que un elemento $y \in Y$ es un **elemento maximal** de Y si no existe otro elemento en Y mayor que él. Es decir,

$$y \in Y \text{ es un elemento maximal} \iff \forall\, z \in Y \mid y \leq z \Rightarrow z = y$$

• Se dice que un elemento $y \in Y$ es un **elemento minimal** si no existe otro elemento en Y menor que él. Es decir,

$$y \in Y \text{ es un elemento minimal} \iff \forall\, z \in Y \mid z \leq y \Rightarrow z = y$$

Ejemplos H *Consideremos los siguientes conjuntos ordenados, A, B, C, D (con los ordenes dados por los grafos respectivos) y los subconjuntos A', B', C', D'.*



Entonces los elementos notables en A', B', C', D' son:

	Cot. Sup.	*Sup.*	*Máx.*	*E. Max.*	*Cot. Inf.*	*Ínf*	*Mín.*	*E. Min*
A'	$\emptyset$	$\emptyset$	$\emptyset$	$\{2, y\}$	1	1	$\emptyset$	$\{2, y\}$
B'	ψ	ψ	$\emptyset$	$\{\beta, \alpha\}$	$\{\mu, \gamma\}$	$\emptyset$	$\emptyset$	$\{\beta, \alpha\}$
C'	b	b	$\emptyset$	$\{e, d\}$	$\{f\}$	$\emptyset$	f	$\{f\}$
D'	3	$\emptyset$	3	$\{3\}$	$\{1, 2\}$	$\emptyset$	2	$\{2\}$

Fin de clase 6 (día 11 problemas) y 7; 13-10-2011, grupo A y B. Día 7 inauguración del curso

Definición 15 Se dice que un conjunto ordenado $(X, \leq)$ es un **retículo** si para todo par de elementos $a, b \in X$ existe $\text{Sup}(\{a, b\})$.

Ejemplos I

⋆ *de los conjuntos ordenados A, B, C, D sólo C y D son retículos. Ya que en A no existe el supremo de $\{2, y\}$ y en B no existe el supremo de $\{\mu, \gamma\}$.*

⋆ *Si X es un conjunto y sea $(\mathcal{P}(X), \subseteq)$ el conjunto ordenado "partes de X" con la relación de orden "contenido", ver el ejemplo G ($\star_2$) (Pag. 18). Entonces el supremo de dos elementos $A, B \subset X$ es $A \cup B$ (por tanto $(\mathcal{P}(X), \subseteq)$ es un retículo). Mientras que el ínfimo de dos elementos $A, B \subset X$ es $A \cap B$.*

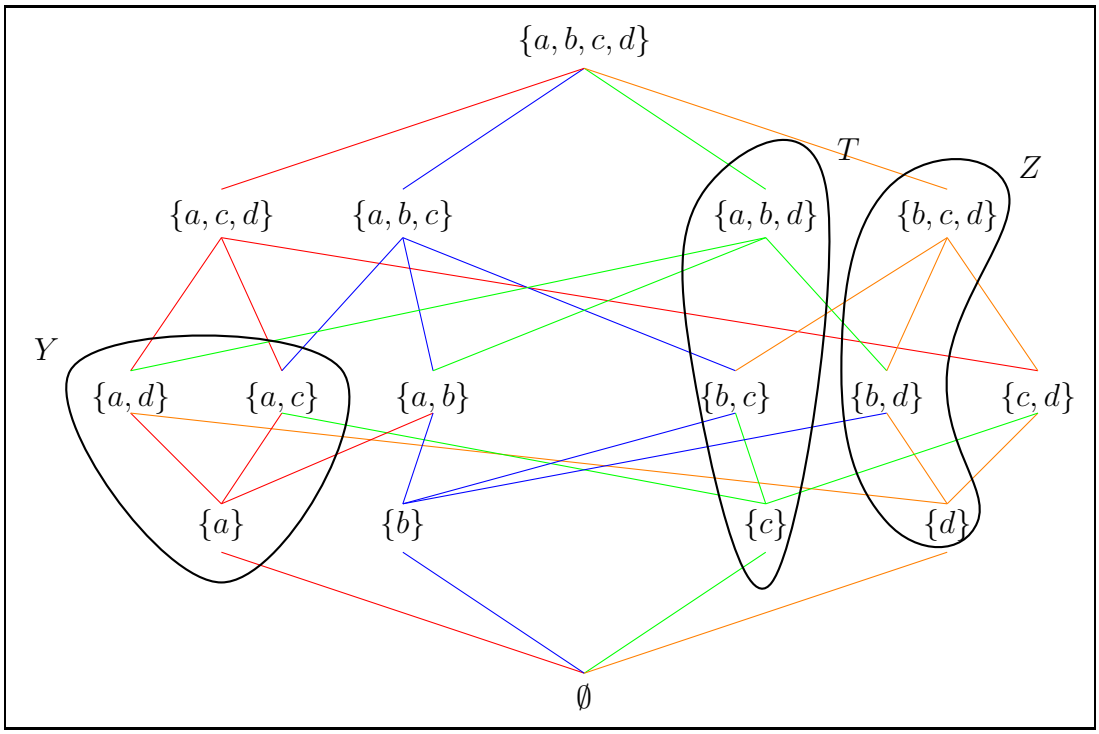
Definición 16 Se dice que un conjunto ordenado $(X, \leq)$ posee un **buen orden** si todo subconjunto no vacío de X posee un elemento mínimo.

• Los Naturales con su orden usual, $(\mathbb{N} \leq)$, es un conjunto ordenado que posee un buen orden.

Definición 17 Sea $(X, \leq)$ un conjunto ordenado. Un subconjunto Y de X es una **cadena** si está totalmente ordenado, es decir, cualquier par de elementos de Y son comparables.

Ejemplos J Consideremos $X = \{a, b, c, d\}$ y sea $(\mathcal{P}(X), \subseteq)$ el conjunto ordenado "partes de X" con la relación de orden "contenido". Sean

$$Y := \{\{a\}, \{a, c\}, \{a, d\}\},\ Z := \{\{d\}, \{b, d\}.\{b, c, d\}\},\ T := \{\{c\}, \{b, c\}, \{a, b, d\}\}.$$



Tenemos entonces:

- Z es una cadena en $\mathcal{P}(X)$, mientras que Y y T no lo son.
- Las cotas superiores de Z son $\{b,c,d\}$ y X. Tiene máximo, $\text{Max}(Z) = \{b,c,d\}$. Las cotas inferiores de Z son $\{d\}$ y $\emptyset$, El ínfimo de Z es su mínimo, $\text{Min}(Z) = \{d\}$. Es más, $\{d\}$ es el único elemento minimal de Z, mientras que $\{b,c,d\}$ es su único elemento maximal.
- Las cotas superiores de Y son $\{a,c,d\}$ y X. Tiene supremo, $\text{Sup}(Y) = \{a,c,d\}$, que no es máximo. Las cotas inferiores de Y son $\{a\}$ y $\emptyset$, El ínfimo de Y es su mínimo, $\text{Min}(Y) = \{a\}$. Es más, $\{a\}$ es el único elemento minimal de Y, mientras que $\{a,c\}$ y $\{a,d\}$ son elementos maximales.
- La cota superior de T es X. Tiene supremo, $\text{Sup}(T) = X$, que no es máximo. La cota inferior de T es $\emptyset$, El ínfimo de T es $\text{Inf}(T) = \emptyset$. Es más, $\{c\}$ y $\{a,b,d\}$ son elementos minimales, mientras que $\{b,c\}$ y $\{a,b,d\}$ son maximales.

Definición 18 Se dice que un conjunto ordenado $(X, \leq)$ es **inductivo** si toda cadena de X admite una mayorante.

Lema 19 (Lema de Zorn) Todo conjunto inductivo posee elementos maximales.

El Lema de Zorn es un axioma, por lo que no es demostrable. No hay conformidad total, en el mundo matemático, a la hora de aceptar este axioma: hay matemáticos que lo aceptan (y lo usan) y otros que no. El no aceptarlo conlleva ciertas consecuencias: no es posible demostrar, sin el axioma de Zorn, que todo espacio vectorial posea una base (no obstante, nadie ha encontrado hasta el momento una base para el espacio vectorial de las sucesiones reales, o una base de $\mathbb{R}$ como $\mathbb{Q}$ espacio vectorial). Si está demostrado que el Lema de Zorn es equivalente a los siguientes resultados:

Lema 20 (Principio de elección) Dada una familia no vacía de conjuntos no vacíos $\{X_i\}$ con $i \in I$, es posible elegir un elemento de cada conjunto. O lo que es equivalente, el producto cartesiano de una familia no vacía de conjuntos no vacíos es no vacío (aunque en este momento no sepáis que es un producto cartesiano de un producto infinito de conjuntos).

Lema 21 (Lema de Zermelo) Todo conjunto no vació admite un buen orden.

Hago notar que nadie ha sabido dar una estructura de buen orden en el conjunto de los Números Reales. No obstante, este resultado permite usar el llamado **principio de inducción transfinito**, por tanto, quien no acepte el lema de Zorn, no puede usar dicho principio.

★ Los ejercicios del 19 al 26 de este tema pueden servirte para comprobar si has asimilado las nociones de esta sección.

4. Cardinales

Cuando contamos los elementos de un conjunto X con n elementos, lo que hacemos (por si no nos hemos dado cuenta) es ponerlo en correspondencia biyectiva con el conjunto $\{1, 2, \ldots, n\}$. En este caso diremos que X es un conjunto con n elementos o que tiene cardinal n. Cuando el conjunto es infinito la noción "tener el mismo número de elementos" se complica un poco:

Podríamos pensar que el conjunto de los números naturales, $\mathbb{N}$, tiene "más" elementos que el conjunto de los número naturales que son pares, vamos a denotar este conjunto por $\mathbb{P}$. No obstante, la aplicación $f : \mathbb{N} \to \mathbb{P}$ definida por $f(n) = 2n$ es biyectiva (lo que nos hace suponer que tienen el mismo número de elementos.

Definición 1 Se dice que dos conjuntos X e Y son **equipotentes** si existe una aplicación biyectiva $f : X \to Y$.

Lema 2 La relación "ser equipotente a" verifica las propiedades reflexiva, transitiva y simétrica.

Nota: Queremos definir el cardinal de un conjunto, con la idea de que dos conjuntos X e Y tienen el mismo cardinal si son equipotentes (existe una biyección $f : X \to Y$). Es decir, si pertenecen a la misma clase de equivalencia de la relación "ser equipotente a".

No podemos dar un nombre a cada uno de los cardinales, aunque algunos tienen nombre propio.

Definición 3 Se define el cardinal de un conjunto X y se denota por $|X|$ o $\#X$ como la clase de equivalencia de X en la relación "ser equipotente a" (es decir, como la clase de todos los conjuntos que son equipotentes a X).

Nota: Observar que con esta definición dos conjuntos tienen el mismo cardinal si y sólo si son equipotentes.

Alguna de estas clases de equivalencia tienen nombre propio:

- El cardinal del conjunto vacío se denota por 0.

- Diremos que un conjunto no vació X es **finito** de cardinal n si X es equipotente al conjunto $\{1, 2, \ldots, n\}$, denotado por $|X| = n$. En caso contrario diremos que X es de cardinal **infinito**, denotado por $|X| = \infty$.
- El cardinal de los números Naturales se representa por $\aleph_0$, que se lee aleph sub cero.
- El cardinal de los números Reales se denota por $\aleph_1$, que se lee aleph sub uno.

Nota: Se vera en ejercicios que el cardinal de los números racionales, aunque en principio pueda sorprender, es $\aleph_0$. No obstante, no hay un único cardinal infinito, $\mathbb{N}$ y $\mathbb{R}$ no son equipotentes.

Proposición 4 Sea X un conjunto finito y $f : X \to X$ una aplicación. Entonces:

(i) Si f es inyectiva, entonces es sobreyectiva.

(ii) Si f es sobreyectiva, entonces es inyectiva. (ejercicio)

Demo: (i) Supongamos que f es inyectiva. Dado $x \in X$ consideramos el conjunto

$$\{x, f(x), f^2(x), \ldots, f^n(x), \ldots\} \subset X$$

como todos estos elementos no pueden ser distintos, ya que X es finito, existen $n, m \in \mathbb{N}$, podemos suponer $n < m$, tal que $f^n(x) = f^m(x)$. Pero si $n \geq 1$,

$$f^n(x) = f(f^{n-1}(x)) = f(f^{m-1}(x)) = f^m(x)$$

lo que implica, al ser f inyectiva, que $f^{n-1}(x) = f^{m-1}(x)$. Reiterando este proceso vamos reduciendo la potencia de f por lo que obtenemos $f(x) = f(m - n + 1)(x)$ y por tanto, aplicando una vez más que f es inyectiva, $x = f^{m-n}(x)$. Por último como $m - n > 0$, $f(f^{m-n-1}(x)) = x$ lo que demuestra que x es la imagen de $f^{m-n-1}(x)$ y por tanto f es sobreyectiva.

(ii) queda como ejercicio. ■

★ Los ejercicios del 27 al 35 de este tema pueden servirte para comprobar si has asimilado las nociones de esta sección.

5. Ejercicios del Tema

1 Sea $X = \{1, 2, 3, a, b, c, \alpha, \beta, \gamma, \{1, a\}, \{4\}, \{a, b, c\}\}$. Di si las siguientes afirmaciones son ciertas o falsas:

$$\begin{array}{ccccc} a \in X & \{1,a\} \in X & \{1,a\} \subset X & 4 \in X & \{a,b,c\} \subset X \\ 3 \subset X & \{\alpha, \{4\}\} \subset X & \{4\} \subset X & X \subset X & \{a,b,c\} \in X \end{array}$$

2 Di si los siguientes son conjuntos. Caso de ser conjuntos, da una descripción alternativa de ellos: *

- $\{x \in \mathbb{R} \mid x^2 = 2\}$.
- $\{x \in \mathbb{R} \mid x^2 < 0\}$.
- $\{x \in \mathbb{Q} \mid x = \frac{n}{m} \text{ con } n, m \in \mathbb{N}, m > 100\}$.
- $\{x \in \mathbb{Q} \mid x \text{ se puede escribir de la forma } \frac{n}{m} \text{ con } n, m \in \mathbb{N}, m > 100\}$.
- $\{x \in \mathbb{Q} \mid x = \frac{n}{m} \text{ con } n, m \in \mathbb{N}, m = 3\}$.

3 Sea X un conjunto y A, B y C tres subconjuntos de X. Demuestra que si $A \cap C = B \cap C$ y $A \cup C = B \cup C$ entonces $A = B$.

4 Sean X e Y dos conjuntos. Da una condición necesaria y suficiente para que los conjuntos $X \times Y$ e $Y \times X$ sean disjuntos.

5 Sean $A_n = \{k \in \mathbb{N} \mid k \neq n\}$. Calcula $\cap_n A_n$, $\cup_n A_n$, $\cap_n \overline{A}_n$ y $\cup_n \overline{A}_n$ en donde $\overline{A}_n$ significa el complemento de A_n en $\mathbb{N}$.

6 Sean X e Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación. Demuestra que para todo par de subconjuntos $A, B \subset X$,

- Si $A \subset B$, entonces $f(A) \subset f(B)$.
- $f(A \cup B) = f(A) \cup f(B)$.
- $f(A \cap B) \subset f(A) \cap f(B)$.

7 Sean X e Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación. Demuestra que f es inyectiva si y sólo si para todo $A, B \subset X$ se verifica que $f(A \cap B) = f(A) \cap f(B)$ *

8 Sean X, Y y Z tres conjuntos no vacíos y $f : X \to Y$, $g : Y \to Z$ dos aplicaciones. Demuestra:

- Si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.
- Si $g \circ f$ es inyectiva, entonces f es inyectiva. ¿Será g inyectiva?

9 Da un ejemplo de tres conjuntos no vacíos X, Y y Z y dos aplicaciones $f : X \to Y$, $g : Y \to Z$ tales que $g \circ f$ sea inyectiva pero g no sea inyectiva.

10 Da un ejemplo de tres conjuntos no vacíos X, Y y Z y dos aplicaciones $f : X \to Y$, $g : Y \to Z$ tales que $g \circ f$ sea sobreyectiva pero f no sea sobreyectiva.

11 Sea X un conjunto no vacío y $f, g, h : X \to X$ tres aplicaciones. Supongamos que $f \circ g = \mathrm{Id}_X = h \circ f$. Demuestra que $h = g$.

12 Sean X, Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación. Demuestra:

- f es inyectiva si y sólo si para todo $y \in Y$ se tiene que $\#f^{-1}(\{y\}) \leq 1$.
- f es sobreyectiva si y sólo si para todo $y \in Y$ se tiene que $\#f^{-1}(\{y\}) \geq 1$.

13 Sean X e Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación sobreyectiva. Demuestra que existe una aplicación inyectiva $g : Y \to X$.

14 Sean X, Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación. Consideremos la aplicación $\Psi : \mathcal{P}(X) \to \mathcal{P}(Y)$ definida por $\Psi(A) = f(A)$ (para cada $A \subset X$, ver la definición 4 (Pag. 8)). Supongamos que existe un subconjunto $D \subset Y$ tal que para cada subconjunto no vació $A \subset X$ se tiene que $\Psi(A) = D$. Demuestra que f es una aplicación constante. Demuestra que el cardinal de D es 1. $\boxed{*}$

15 Sean X, Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación. Consideremos la aplicación $\Phi : \mathcal{P}(Y) \to \mathcal{P}(X)$ definida por $\Psi(B) = f^{-1}(B)$ (para cada $B \subset Y$, ver la definición 4 (Pag. 8)). Supongamos que para cada subconjunto $B \subset Y$ se tiene que $\Phi(B) = X$ o $\Phi(B) = \emptyset$. Demuestra que f es una aplicación constante. $\boxed{*}$

16 Sean X, Y dos conjuntos no vacíos. En la definición 4 (Pag. 8) se ha construido una aplicación $\Phi_f : \mathcal{P}(X) \to \mathcal{P}(Y)$ para cada aplicación $f : X \to Y$. Encuentra una aplicación $\Phi : \mathcal{P}(X) \to \mathcal{P}(Y)$ tal que no exista ninguna aplicación $f : X \to Y$ con $\Phi = \Phi_f$. $\boxed{*}$

17 Sean X, Y dos conjuntos no vacíos. En la definición 4 (Pag. 8) se ha construido una aplicación $\Psi_f : \mathcal{P}(Y) \to \mathcal{P}(X)$ para cada aplicación $f : X \to Y$. Encuentra una aplicación $\Psi : \mathcal{P}(Y) \to \mathcal{P}(X)$ tal que no exista ninguna aplicación $f : X \to Y$ con $\Psi = \Psi_f$. $\boxed{*}$

18 Sean X e Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación.

- Demuestra que la relación $a \mathcal{R} b$ si y sólo si $f(a) = f(b)$ es de equivalencia en X.
- Calcula las clases de equivalencia para la aplicación dada en el ejemplo C (Pag. 8).
- ¿Que propiedad debe de cumplir $\mathcal{R}$ para que f sea inyectiva? ¿Se puede caracterizar la sobreyectividad de forma similar? $\boxed{*}$

19 Sea $\mathbb{N}$ el conjunto de los número naturales. Demuestra que la relación $n \mathcal{R} m$ si y sólo si $n - m$ es múltiplo de 7 es de equivalencia. Calcula el conjunto cociente.

20 La propiedad reflexiva es redundante en una relación de equivalencia: si $a \mathcal{R} b$ por la propiedad simétrica $b \mathcal{R} a$ y por la transitiva $a \mathcal{R} a$. ¿Donde está el error? $\boxed{*}$

21 Dados dos elementos $a, b \in \mathbb{N}$ diremos que a divide a b y lo representamos por ${}^{a}|_{b}$ si existe $c \in \mathbb{N}$ tal que $b = ca$. Demuestra que la relación de divisibilidad es una relación de orden en $\mathbb{N}$. Calcula los elementos notables para $Y = \{2, 3, 4, 5, 6, 7, 8\}$ y para $Z = \{14, 21\}$.

22 Sea X un conjunto no vacío y consideremos el conjunto ordenado $(\mathcal{P}(X), \subset)$. Sea $\{A_i\}_{i\in I}$ una familia de subconjuntos. ¿Quien es $\text{Sup}(\{A_i\}_{i\in I})$ e $\text{Inf}(\{A_i\}_{i\in I})$? ¿Son respectivamente máximo y mínimo?

23 Demuestra que en un retículo existe el supremo de cualquier subconjunto finito. **Nota:** Demuestra que $\boxed{*}$

$$Sup\{A_1, \ldots, A_{n-1}, A_n\} = Sup\{Sup\{A_1, \ldots, A_{n-1}\}, A_n\}$$

24 Sea $(X, \leq)$ un conjunto ordenado tal que todo subconjunto de X posee un único elemento minimal. Demuestra que X posee un buen orden. $\boxed{*}$

25 Sean $(X, \leq)$ y $(X', \leq')$ dos conjuntos ordenados y sea $f : X \to X'$ una aplicación sobreyectiva tal que para todo $a, b \in X$, si $a \leq b$, entonces $f(a) \leq f(b)$. ¿Es cierto que si X es un retículo, X' también es un retículo?. $\boxed{*}$

No

26 Encuentra un conjunto ordenado en donde todo subconjunto posea máximo. ¿Puedes encontrarlo con un subconjunto que no posea mínimo?

27 Sean $\{X_i\}$ con $i = 1, 2, \ldots, n$ una familia de conjuntos no vacíos. Demuestra que el conjunto

$$\{f : \{1, 2, \ldots, n\} \to \bigcup_{i=1}^{n} X_i \mid f(i) \in X_i \text{ para todo i}\}$$

es un conjunto equipotente a $X_1 \times X_2 \times \cdots \times X_n$. $\boxed{*}$

28 Sean X e Y dos conjuntos no vacíos. Demuestra que $X \times Y$ e $Y \times X$ tienen el mismo cardinal.

29 Demuestra que $\mathbb{N}$ y $\mathbb{Q}$ tienen el mismo cardinal. $\boxed{*}$

30 Demuestra que $\mathbb{N}$ y $\mathbb{R}$ no son equipotentes. $\boxed{*}$

31 Sean X e Y dos conjuntos equipotentes. Sea $x_0 \in X$ y $y_0 \in Y$. Demuestra que $X - \{x_0\}$ e $Y - \{y_0\}$ son también equipotentes.

32 Demuestra que $\mathbb{R}$ es equipotente a $\mathbb{R} - \{0\}$.

33 Sean X e Y dos conjuntos no vacíos. Supongamos que hay una aplicación inyectiva $f : X \to Y$ y una aplicación inyectiva $g : Y \to X$. Entonces existe una aplicación biyectiva $h : X \to Y$. (Ejercicio muy complicado, hace uso del lema de Zorn [puede ser encontrado en internet]) $\boxed{***}$

• Es lógico pensar que si tenemos una aplicación inyectiva $f : X \to Y$ es porque en X hay menos ($\leq$) elementos que en Y. Luego este ejercicio dice que si en X hay menos ($\leq$) elementos que en Y y en Y hay menos ($\leq$) elementos que en X es porque X e Y tienen el mismo número de elementos

34 *Puede existir un conjunto X que verifique la siguiente propiedad: Para todo elemento $a \in X$ se verifica que $a \subset X$.* ***Observar*** *que esta propiedad, en particular, dice que todo los elementos de X son conjuntos.* $\boxed{**}$

35 *Puede existir un conjunto X que verifique la siguiente propiedad: Para todo subconjunto $A \subset X$ se verifica que $a \in X$.*

36 *Sean X, Y, Z, T cuatro conjuntos. Sea $f : X \to Y$ y $g : Z \to T$ dos aplicaciones. Sea $z_0 \in Z$ y $ct_{z_0} : Y \to Z$ la aplicación constante (para todo $y \in Y$, $ct_{z_0}(y) = z_0$). Demuestra que las aplicaciones*

$$ct_{z_0} \circ f : X \to Z \quad y \quad g \circ ct_{z_0} : Y \to T$$

son también aplicaciones constantes. ¿Son $ct_{z_0} : Y \to Z$ y $ct_{z_0} \circ f : X \to Z$ la misma aplicación?

37 Sean X, Y dos conjuntos no vacíos. En la definición 4 (Pag. 8) se ha construido una aplicación $\Phi_f : \mathcal{P}(X) \to \mathcal{P}(Y)$ para cada aplicación $f : X \to Y$. ¿Si f es una aplicación inyectiva (sobreyectiva), Φ_f es también inyectiva(sobreyectiva)?.

38 Sean X, Y dos conjuntos no vacíos. En la definición 4 (Pag. 8) se ha construido una aplicación $\Psi_f : \mathcal{P}(Y) \to \mathcal{P}(X)$ para cada aplicación $f : X \to Y$.¿Si f es una aplicación inyectiva (sobreyectiva), Ψ_f es también inyectiva (sobreyectiva)?.

Capítulo 2

Los Naturales y los Enteros.

Objetivos del capítulo

- Introducir los Números Naturales y los Números Enteros estudiando sus propiedades respecto de la suma, del producto y del orden. Especialmente el principio de inducción e inducción generalizado.
- Estudio y aplicación del algoritmo de la división. Existencia y unicidad del m. c. d y M. C. M. Teorema de Bezout y factorización única en $\mathbb{Z}$.
- Estudio de los anillos de congruencias módulo n.

---

1. Los Números Naturales y los Números enteros

1.1. Los Números Naturales

Definición 1 Los Números Naturales aparecen por la necesidad que tiene el hombre (primitivo) tanto de contar como de ordenar una cierta cantidad de objetos.

$$\mathbb{N} := \{1, 2, 3, \dots\}$$

En los números naturales podemos sumar y multiplicar, pero no podemos, en la mayoría de los casos, ni restar ni dividir. Históricamente el cero no es considerado un número natural. Matemáticamente los naturales se definen a partir de 5 axiomas, los **Axiomas de Peano**:

1). El 1 es un número natural.

2). Para cada número natural n existe otro número natural n'.

3). Si $n \in \mathbb{N}$, $n' \neq 1$.

4). Si $n, m \in \mathbb{N}$ y $n' = m'$, entonces $n = m$.

5). **Principio de inducción matemática**: Si S es un subconjunto de $\mathbb{N}$ tal que:

   a) $1 \in S$ y

b) si $n \in S$, entonces $n' \in S$. Se tiene que $S = \mathbb{N}$

Nota: Observar que, en la representación usual de los Naturales, para cada $n \in \mathbb{N}$, n' no es más que $n + 1$.

Primera vez que se usa el principio de inducción

Ejemplos A Demuestra que para todo número natural n se verifica que

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Demo: Consideremos el conjunto S de los números naturales para los que la igualdad es cierta. Es claro que $1 \in S$, ya que $1 = 1^2$. Supongamos que la igualdad es cierta para n, es decir que $n \in S$ y veamos que es cierta para $n + 1$. Tenemos, por hipótesis, que

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

Observar que el siguiente impar de $2n - 1$ es $2n + 1$, por tanto, si sumamos en ambos lados de la igualdad $2n + 1$ obtenemos

$$1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = n^2 + 2n + 1 = (n + 1)^2$$

es decir, que $n+1 \in S$. Por tanto aplicando el principio de inducción matemática, $S = \mathbb{N}$, lo que demuestra que la igualdad es cierta para todo número natural. ■

Definición 2 (Principio de inducción generalizado:) Sea S un subconjunto de $\mathbb{N}$ tal que:

- $1 \in S$ y
- si $1, 2, \ldots, n \in S$, entonces $n + 1 \in S$.

Entonces $S = \mathbb{N}$

En este punto nos separamos de la teoría axiomática de los Números Naturales (tanto la suma, el producto como el buen orden de $\mathbb{N}$ se pueden definir usando una pequeña cantidad de axiomas; a partir de ellos se pueden demostrar todas las propiedades que vamos a ver a continuación). Si quieres ver la teoría completa, la puedes encontrar en [1].

Definición 3 (Propiedades de los Números Naturales)

1. Propiedades respecto de la suma:
   a) Propiedad asociativa: $(x + y) + z = x + (y + z) \quad \forall\, x, y, z \in \mathbb{N}$.
   b) Existencia de elemento neutro: $x + 0 = 0 + x = x \quad \forall\, x \in \mathbb{N}$. (si $0 \in \mathbb{N}$)
   c) Propiedad conmutativa: $x + y = y + x \quad \forall\, x, y \in \mathbb{N}$.
2. Propiedades respecto del producto:

a) Propiedad asociativa: $(x\,y)\,z = x\,(y\,z) \quad \forall\, x, y, z \in \mathbb{N}$.

b) Existencia de elemento neutro: $x\,1 = 1\,x = x \quad \forall\, x \in \mathbb{N}$.

c) Propiedad conmutativa: $x\,y = y\,x \quad \forall\, x, y \in \mathbb{N}$.

d) Ley de simplificación: $\forall\, x, y, z \in \mathbb{N}$, con $x \neq 0$, si $x\,y = x\,z$, entonces $y = z$.

3. Propiedades respecto del orden: **Los Naturales poseen un buen orden**, es decir, cualquier subconjunto no vacío de $\mathbb{N}$ posee elemento mínimo.

4. Propiedades conjuntas: para todo $x, y, z \in \mathbb{N}$

a) Propiedad distributiva: $(x + y)\,z = x\,z + y\,z$.

b) Si $x \leq y$, entonces $x + z \leq y + z$.

c) Si $x \leq y$, entonces $xz \leq yz$.

Nota: Dado $(X, \leq)$ cualquier conjunto ordenado y dados $x, y \in X$ denotamos por:

- $x < y$, que se leerá x menor estricto que y, si $x \leq y$ con $x \neq y$.
- $x \geq y$, que se leerá x mayor o igual que y, si $y \leq x$.
- $x > y$, que se leerá x mayor estricto que y, si $y \leq x$ con $y \neq x$.

En particular, para $(\mathbb{N}, \leq)$ tenemos que, $1 \leq x$ para todo $x \in \mathbb{N}$, con lo que $1 < x$ siempre que $1 \neq x$.

1.2. Los Números Enteros

Definición 4 Los Números Enteros: aparecen simetrizando el conjunto de números naturales, y añadiéndoles el cero. Los denotaremos por $\mathbb{Z}$. Con este nuevo conjunto de números obtenemos la mejoría de que, ahora sí, la resta de dos números enteros es un número entero.

$$\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Definición 5 (Propiedades de los Números Enteros)

1. Propiedades respecto de la suma:

a) Propiedad asociativa: $(x + y) + z = x + (y + z) \quad \forall\, x, y, z \in \mathbb{Z}$.

b) Existencia de elemento neutro: $x + 0 = 0 + x = x \quad \forall\, x \in \mathbb{Z}$.

c) Existencia de elemento opuesto: para todo $x \in \mathbb{Z}$ existe $-x \in \mathbb{Z}$ tal que

$$x + (-x) = (-x) + x = 0.$$

d) Propiedad conmutativa: $x + y = y + x \quad \forall\, x, y \in \mathbb{Z}$.

2. Propiedades respecto del producto:

a) Propiedad asociativa: $(x\,y)\,z = x\,(y\,z) \quad \forall\, x, y, z \in \mathbb{Z}$.

b) Existencia de elemento neutro: $x\,1 = 1\,x = x \quad \forall\, x \in \mathbb{Z}$.

c) Propiedad conmutativa: $x\,y = y\,x \quad \forall\ x, y \in \mathbb{Z}$.

d) Ley de simplificación: $\forall\ x, y, z \in \mathbb{Z}$, con $x \neq 0$, si $x\,y = x\,z$, entonces $y = z$.

3. Propiedades conjuntas:

   a) Propiedad distributiva: $(x + y)\,z = x\,z + y\,z \quad \forall\ x, y, z \in \mathbb{Z}$.

4. Propiedades respecto del orden: para todo $x, y, z \in \mathbb{Z}$

   a) Si $x \leq y$, entonces $x + z \leq y + z$.

   b) Si $x \leq y$ y $0 \leq z$, entonces $x\,z \leq y\,z$.

   c) Si $x \leq y$, y $z \leq 0$, entonces $y\,z \leq x\,z$.

Nota: Observar que normalmente los elementos de $\mathbb{Z}$ no poseen inverso.

Definición 6 Se define el **valor absoluto** de un número entero $x \in \mathbb{Z}$ y se representa por $|x|$ como:

$$|x| := \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}$$

★ Los ejercicios del 1 al 6 te pueden servir para saber si has asimilado los conceptos de esta sección.

Fin de clase 8; 14-10-2011, grupo A y B

2. Factorización y Divisibilidad en $\mathbb{Z}$

2.1. Algoritmo de la División y Divisibilidad en $\mathbb{Z}$

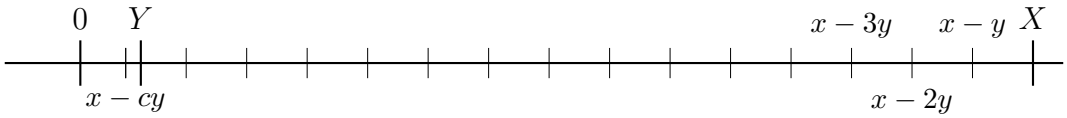
Proposición 1 (Algoritmo de la división.) Dados dos números enteros $x, y \in \mathbb{Z}$ con $y > 0$ existen $c, r \in \mathbb{Z}$ (únicos), tales que $x = cy + r$ con $0 \leq r < y$.

la primera vez que se usa reducción al absurdo.

Demo: Consideremos el conjunto

$$X := \{x - ny \mid x - ny \geq 0,\ n \in \mathbb{Z}\} \subset \mathbb{N}$$

Gráficamente tenemos:



Es claro que $X \neq \emptyset$, ya que:

– Si $x \geq 0$, $\quad x = x - 0y \in X$ y,

– Si $x \leq 0$, $\quad 0 \leq x(1-y) = x - (xy) \in X$.

Por tanto, aplicando que $(\mathbb{N}, \leq)$ es un buen orden, sea $r = \text{Min}(X)$. Así, existe $c \in \mathbb{Z}$ tal que $r = x - cy$, es decir, $x = cy + r$. Veamos ahora que $r < y$. Por reducción al absurdo, si $y \leq r$, tenemos que $0 \leq r - y = x - (c+1)y \in X$, una contradicción, ya que $r - y < r$ y r era el mínimo en X. Por tanto, hemos encontrado $c, r \in \mathbb{Z}$ tales que $x = cy + r$ con $0 \leq r < y$.

Veamos, por último, que c y r son únicos: Supongamos r, r', c, c' tales que

$$\begin{aligned} x &= cy + r \qquad 0 \leq r < y \\ x &= c'y' + r' \qquad 0 \leq r' < y \end{aligned}$$

Podemos suponer $0 \leq r \leq r' < y$. Entonces $cy + r = c'y + r'$ por lo que

$$0 \leq r' - r = (c - c')y. \tag{1}$$

Por tanto, $r' - r$ es múltiplo de y y $r' - r \leq r' < y$, con lo que la única posibilidad es $r' - r = 0$, ver el ejercicio 5 (Pag. 48). Ahora, por la ley de simplificación $c - c' = 0$. ■

Proposición 2 (Algoritmo de la división (ejercicio).) Dados dos números enteros $x, y \in \mathbb{Z}$ con $y \neq 0$ existen $c, r \in \mathbb{Z}$ (únicos), tales que $x = cy + r$ con $0 \leq r < |y|$.

Definición 3 Con la notación del teorema anterior se dice que x es el **dividendo**, y el **divisor**, c el **cociente** y r el **resto**.

Definición 4 Sean x, y dos números enteros. Se dice que y **divide** a x y se representa ${}^{y}|_{x}$ si existe $c \in \mathbb{Z}$ tal que $x = cy$.

Corolario 5 (Ejercicio 8 (Pag. 48)) La relación de divisibilidad en $\mathbb{Z}$ es reflexiva, transitiva y verifica que para todo $a, b \in \mathbb{Z}$, si

$${}^{a}|_{b} \text{ y } {}^{b}|_{a} \quad \text{entonces } a = \pm b.$$

Por tanto, es una relación de orden en $\mathbb{N}$.

2.2. Máximo Común divisor

Definición 6 Sean x e y dos número enteros alguno de ellos no nulo. Se define el **máximo común divisor** de x e y, y se representa por $\text{m. c. d}(x, y)$ como un número $d \in \mathbb{Z}$ con las siguientes propiedades:

1. $d > 0$.
2. ${}^{d}|_{x}$ y ${}^{d}|_{y}$.
3. Si ${}^{r}|_{x}$ y ${}^{r}|_{y}$, entonces ${}^{r}|_{d}$.

Proposición 7 Sean x, y dos enteros alguno no nulos. Entonces existen $\mathrm{m.c.d}(x, y)$ y es único. Es más, existen $r, s \in \mathbb{Z}$ tales que $rx + sy = m.c.d(x, y)$.

Demo: Sea el conjunto

$$X = \{ax + by \mid a, b \in \mathbb{Z}, \text{ con } ax + by > 0\} \subset \mathbb{N}.$$

Es claro que $X \neq \emptyset$, ya que $x^2 + y^2 \in X$. Por tanto, aplicando que $(\mathbb{N}, \leq)$ posee un buen orden, existe

$$d = rx + sy = \mathrm{Min}(X) \in \mathbb{N}. \tag{1}$$

Veamos que $d = \mathrm{m.c.d}(x, y)$: por definición, $d > 0$. demostremos que d divide a x. Aplicando el algoritmo de la división a x, d, existen $c, r \in \mathbb{Z}$ tal que $x = cd + r$ con $0 \leq r < d$. Por tanto, $x = c(rx + sy) + r$, luego $r = (1 - cr)x + (-cs)y$. Así, si $r \neq 0$, $r \in X$ con $r < d$, que es imposible. Luego $r = 0$, o lo que es lo mismo, d divide a x. Cambiando los papeles de x e y demostramos que d divide a y. Por último, Si a divide a x y divide a y, entonces $x = ax'$, $y = ay'$ y por tanto $d = rx+sy = rax'+say' = (rx'+sy')a$ lo que demuestra que a divide a d.

Veamos la unicidad: si d y d' verifican las propiedades de $\mathrm{m.c.d}(x, y)$, entonces ${}^{d}|_{d'}$ y ${}^{d'}|_{d}$ por lo que $d = \pm d'$ pero como ambos son números naturales, tenemos que $d = d'$. ■

Nota: Observar que hemos conseguido, a partir de una demostración indirecta, demostrar que existen dos enteros r, s tales que $rx + sy = \mathrm{m.c.d}(x, y)$. Es más, el máximo común divisor de x e y es el menor natural que puede ser escrito en esta forma. No obstante, en un caso concreto, no sabemos encontrar dichos números. El siguiente teorema, debido a Euclides, nos da un algoritmo para calcularlos.
Nota: Aunque pueda parecer una demostración extraña, cuando estudiemos la noción de ideal y los ideales de $\mathbb{Z}$ veremos que el resultado (y su demostración) son muy obvios.
Nota: En ningún momento se ha dicho que r y s sean únicos. Así: $\mathrm{m.c.d}(2, 3) = 1$ y,

$$\begin{aligned} 1 \quad &\cdot 3 + (-1) \cdot 2 = 1 \\ (-3) \cdot 3 + \quad &5 \quad \cdot 2 = 1. \end{aligned}$$

Lema 8 (Ejercicio 7 (Pag. 48)) *Sean $x, y, a, b \in \mathbb{Z}$, Entonces:*

(i) Si ${}^{x}|_{y}$, entonces $\mathrm{m.c.d}(x, y) = |x|$.

(ii) Si ${}^{x}|_{a}$ y ${}^{x}|_{b}$, entonces ${}^{x}|_{\alpha a+\beta b}$ para todo $\alpha, \beta \in \mathbb{Z}$.

Teorema 9 (Algoritmo de Euclides) Sean x, y dos enteros no nulos. Supongamos que $x = cy + r$ con $r \neq 0$. Entonces

(i) $\mathrm{m.c.d}(x, y) = \mathrm{m.c.d}(y, r)$.

(ii) Aplicando el algoritmo de la división a x e y: $x = cy + r_1$. Si $r_1 \neq 0$ volvemos a aplicar el algoritmo de la división a y y r_1: $y = c_2 r_1 + r_2$, y reiterando el proceso:

$$\begin{aligned} x &= c_1 y + r_1 \quad \text{si} \quad r_1 \neq 0 \\ y &= c_2 r_1 + r_2 \quad \text{si} \quad r_2 \neq 0 \\ r_1 &= c_3 r_2 + r_3 \quad \text{si} \quad r_3 \neq 0 \\ &\vdots \\ r_k &= c_{k+2} r_{k+1} + r_{k+2} \quad \dots \end{aligned}$$

$\exists\, n \in \mathbb{N}$ tal que $r_n = 0$, entonces $r_{n-2} = c_n r_{n-1}$ y $\text{m. c. d}(x, y) = r_{n-1}$.

Demo: (1). Sea $d = \text{m. c. d}(x, y)$ y $d' = \text{m. c. d}(y, r)$.

$$x = cy + r \tag{1}$$

Como ${}^{d}|_{x}$, ${}^{d}|_{y}$ y $r = x - cy$, ${}^{d}|_{r}$. Ahora, aplicando que $d' = \text{m. c. d}(y, r)$, ${}^{d}|_{d'}$. Análogamente, como d' divide a y y a r, por (1), d' divide a x y por tanto ${}^{d'}|d$. Así, $d = \pm d'$ y por tanto $d = d'$.

(2). La cadena decreciente de números naturales $r_1 > r_2 > r_3 \cdots > r_k > \cdots$ debe de llega a cero (principio del buen orden). Supongamos que $r_n = 0$, entonces $r_{n-2} = c_{n-1} r_{n-1}$. Ahora, aplicando reiteradamente el apartado anterior

$$\text{m. c. d}(x, y) = \text{m. c. d}(r_{n-2}, r_{n-1}) = r_{n-1}$$

■

Ejemplos A Calcula $\text{m. c. d}(1567, 4763)$.

$$\begin{aligned} 4763 &= 3 \cdot 1567 + 62 && (2.1) \\ 1567 &= 25 \cdot 62 + 17 && (2.2) \\ 62 &= 3 \cdot 17 + 11 && (2.3) \\ 17 &= 1 \cdot 11 + 6 && (2.4) \\ 11 &= 1 \cdot 6 + 5 && (2.5) \\ 6 &= 1 \cdot 5 + \boxed{1} && (2.6) \\ 5 &= 5 \cdot 1 + 0 && (2.7) \end{aligned}$$

Luego $\text{m. c. d}(1567, 4763) = 1$. En cualquier caso, observar que rápidamente nos encontramos con números pequeños a los que les podemos calcular de forma fácil su máximo común divisor, $\text{m. c. d}(62, 17) = 1$.

$\star$ Veamos ahora como calcular $r, s \in \mathbb{Z}$ tales que $r \cdot 1567 + s \cdot 4763 = 1$. Despejamos el 5 de (2.5) y lo sustituimos en (2.6): $6 = 1 \cdot (11 - 6) + 1$,

$$1 = (-1) \cdot 11 + 2 \cdot 6 \tag{♣}$$

Despejamos de (2.4) el 6, y lo sustituimos en (♣), $6 = 17 - 11$:

$$1 = (-1) \cdot 11 + 2 \cdot (17 - 11) = (-3) \cdot 11 + 2 \cdot 17 \tag{♦}$$

Despejamos el 11 de (2.3) y lo sustituimos en (♦):

$$1 = (-3) \cdot (62 - 3 \cdot 17) + 2 \cdot 17 = (-3) \cdot 62 + 11 \cdot 17 \qquad (♠)$$

Despejamos el 17 de (2.2) y lo sustituimos en (♠):

$$1 = (-3) \cdot 62 + 11 \cdot (1567 - 25 \cdot 62) = 11 \cdot 1567 - 278 \cdot 62 \qquad (▲)$$

Por último, despejamos 62 de (2.1) y lo sustituimos en (▲):

$$1 = 11 \cdot 1567 - 278 \cdot (4763 - 3 \cdot 1567) = -278 \cdot 4763 + 845 \cdot 1567 \qquad (★)$$

Definición 10 Se dice que un número entero p es **primo** si $|p| \neq 1$ y sólo es divisible por $\{1, -1, p, -p\}$.

Fin de clase 9; 18-10-2011, grupo A y B

Nota: Como ejemplos de números primos: 2,3,5,7,11,13,17,19,23 o incluso el número 29.996.224.275.833 que es el primo número 10^{12}.

Definición 11 Sean x e y dos número enteros no nulos. Se dice que x e y son **primos relativos** si $\text{m. c. d}(x, y) = 1$.

Corolario 12 (Teorema de Bezout) Sean x, y dos enteros no nulos. Las siguientes condiciones son equivalentes:

(i) x, y son primos relativos.

(ii) existen $r, s \in \mathbb{Z}$ tales que $rx + sy = 1$.

Demo:

$(i) \implies (ii)$. Si x, y son primos relativos, por definición, $\text{m. c. d}(x, y) = 1$ luego por el teorema 7 (Pag. 34) existen $r, s \in \mathbb{Z}$ tal que $rx + sy = 1$.

$(ii) \implies (i)$. Supongamos que existen $r, s \in \mathbb{Z}$ tales que $rx + sy = 1$ y $d = \text{m. c. d}(x, y)$. Como d divide a x y d divide a y, $x = dx'$, $y = dy'$ y por tanto

$$1 = rx + sy = rdx' + sdy' = d(rx' + sy')$$

Por tanto d divide a 1 lo que implica que $d = 1$, ver el ejercicio 6 (Pag. 48). Es decir, x e y son primos relativos. ■

Teorema 13 (Teorema Generalizado de Bezout) Sean $n_1, n_2, \ldots, n_r \in \mathbb{N}$ tales que si $k \in \mathbb{N}$ divide a todo n_i, $k = 1$. Entonces existen $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{Z}$ tales que $\alpha_1 n_1 + \alpha_2 n_2 + \cdots + \alpha_r n_r = 1$.

Demo: Vamos a dar una demostración por inducción a r, el número de elementos que tenemos:

(i). Si $r = 2$ tenemos que este resultado es el teorema de Bezout, por lo que no tenemos nada que demostrar.

(ii). Supongamos que el resultado es cierto para $r-1$ y consideremos r naturales no nulos $n_1, n_2, \ldots, n_r \in \mathbb{N}$ tales que si $k \in \mathbb{N}$ divide a todo n_i, $k = 1$. Sean los naturales $n_1, n_2, \ldots, n_{r-1}$ y sea el conjunto

$$\Delta := \{\lambda \in \mathbb{N} \,|\lambda \text{ divide a todos los } n_i \; i = 1, \ldots, r-1\}$$

Es claro que $1 \in \Delta$ y que todo elemento de Δ es menor que cualquiera de los n_i, por lo que es un conjunto finito. Sea β el mayor elemento de Δ. Tenemos entonces que $n_i = \beta n_i'$ con $n_i' \in \mathbb{Z}$ y que el conjunto $\{n_1', n_2', \ldots, n_{r-1}'\}$ verifica la hipótesis de inducción (si hubiera un γ que dividiera a todos los n_i', $\gamma\beta > \beta$ dividiría a todos los n_i, $i = 1, \ldots, r-1$, una contradicción ya que β era el mayor. Por tanto, aplicando la hipótesis de inducción existen $\alpha_i' \in \mathbb{Z}$ tal que

$$\alpha_1' n_1' + \alpha_2' n_2' + \cdots + \alpha_{r-1}' n_{r-1}' = 1. \qquad (*)$$

Por otro lado $\text{m.c.d}(\beta, n_r) = 1$ ya que si algún natural dividiera a β y a n_r dividiría a todos los n_i (que no puede ser por hipótesis). Luego aplicando el teorema de Bezout existen $a, b \in \mathbb{Z}$ tal que

$$a\beta + bn_r = 1. \qquad (**)$$

Luego por $(**)$, y sustituyendo $(*)$, tenemos:

$$\begin{aligned} 1 &= a\beta + bn_r = a\beta(1) + bn_r = a\beta(\alpha_1' n_1' + \alpha_2' n_2' + \cdots + \alpha_{r-1}' n_{r-1}') + bn_r \\ &= a\alpha_1'\beta n_1' + a\alpha_2'\beta n_2' + \cdots + a\alpha_{r-1}'\beta n_{r-1}' + bn_r \\ &= a\alpha_1' n_1 + a\alpha_2' n_2 + \cdots + a\alpha_{r-1}' n_{r-1} + bn_r \end{aligned}$$

que nos demuestra el resultado. ■

Proposición 14 Sean $n_1, n_2, \ldots, n_k$ números enteros no nulos y $p \in \mathbb{Z}$ un número primo. Supongamos que $^p|_{n_1 n_2 \ldots n_k}$ entonces existe $i \in \{1, 2, \ldots, k\}$ tal que $^p|_{n_i}$.

Demo: Vamos a dar una demostración por inducción a k. Demostremos el caso $k = 2$. Supongamos que p no divide a n_1. Entonces $m.c.d(p, n_1) = 1$ por lo que por el Teorema de Bezout existen $\alpha, \beta \in \mathbb{Z}$ tal que

$$\alpha n_1 + \beta p = 1 \qquad (1)$$

Ahora, como por hipótesis $n_1 n_2 = cp$, multiplicando en (1) por n_2,

$$n_2 = n_2(\alpha n_1 + \beta p) = \alpha(n_1 n_2) + \beta p n_2 = \alpha(cp) + \beta p n_2 = (\alpha c + \beta n_2)p \qquad (2)$$

Por tanto, n_2 es divisible por p.

Supongamos que el resultado es cierto para $k-1$, entonces, si $^p|_{n_1 n_2 \ldots n_k}$, aplicando el caso anterior a los números $(n_1 \ldots n_{k-1})$ y n_k tenemos que, $^p|_{n_1 \ldots n_{k-1}}$ o $^p|n_k$ y por el proceso de inducción, si $^p|_{n_1 \ldots n_{k-1}}$, existe un i tal que $^p|_{n_i}$. Lo que demuestra la proposición. ■

2.3. Factorización en $\mathbb{Z}$

Definición 15 (Teorema de Factorización) Dado un número entero n con $|n| > 1$ existen unos únicos $p_1 < \cdots < p_k$ primos y $n_1, \ldots, n_k \in \mathbb{N}$ tales que $n = \pm p_1^{n_1} \ldots p_k^{n_k}$.

Demo: Es claro que podemos suponer $n \in \mathbb{N}$. Vamos a usar el principio de inducción generalizado: si $n = 2$, ya está factorizado. Supongamos que todo número natural menor que n esta factorizado como producto de primos. Si n es primo, no hay nada que demostrar, caso contrario existen $a, b \in \mathbb{N}$ mayores que 1 tales que $n = ab$. Entonces $a, b < n$ y por hipótesis de inducción, a y b factoriza como producto de primos.

Veamos la unicidad: El caso $n = 2$ es trivial. Por tanto, y aplicando el principio de inducción generalizado puedo suponer que tenemos factorización única para todo natural $< n$. Supongamos $n = p_1^{n_1} \ldots p_k^{n_k} = p_1^{m_1} \ldots p_k^{m_k}$ con $n_i, m_i \in \mathbb{N}$ (puedo suponer que los primos que aparecen en la factorización son los mismos al haber permitido el exponente cero). Reordenando puedo suponer $n_1 \neq 0$ y por tanto n es divisible por p_1. Aplicando el resultado anterior, ${}^{p_1}|_{p_1^{m_1} \ldots p_k^{m_k}}$ y como p_1 no puede dividir a ningún primo que no sea el mismo, $m_1 \geq 1$, Tenemos entonces que $p_1^{n_1 - 1} \ldots p_k^{n_k} = p_1^{m_1 - 1} \ldots p_k^{m_k} < n$, aplicando ahora el proceso de inducción $n_i = m_i$ para todo i. ■

Corolario 16 Sean x, y dos enteros no nulos. Entonces el máximo común divisor de x e y es el producto de los primos comunes elevado al menor exponentes (en sus respectivas factorizaciones).

Corolario 17 (Teorema de Euclides) Existen infinitos primos.

Demo: Vamos a dar una demostración por reducción al absurdo. Supongamos que el número de primos es finito, $p_1, p_2, \ldots, p_k$. Sea $n = p_1 p_2 \cdots p_k + 1 \in \mathbb{Z}$. Tenemos que n se factoriza como producto de primos, sea p uno de estos primos. Entonces n es divisible por p, pero $p_1 p_2 \cdots p_k$ es divisible por p, por tanto 1 es divisible por p, una contradicción (si $1 = p\alpha$, $p = \pm 1$ y no puede ser primo). ■

Fin de clase 10; 20-10-2011, grupo A y B

Definición 18 Sean x, y dos número enteros alguno no nulos. Se define el mínimo común múltiplo de x e y y se representa por $\mathrm{M.C.M}(x, y)$ como un número $m \in \mathbb{Z}$ con las siguientes propiedades:

1. $m > 0$.
2. ${}^{x}|_{m}$ e ${}^{y}|_{m}$.
3. Si ${}^{x}|_{r}$ e ${}^{y}|_{r}$, entonces ${}^{m}|_{r}$.

Demo: Hay que demostrar que tal número existe y es único. Una posible demostración consiste en considerar el conjunto

$$\Delta := \{0 < a \in \mathbb{N} \mid {}^{x}|_{a},\ {}^{y}|_{a}\}$$

Demostrar que es no vacío y que es mínimo de este conjunto, digamos m, es el $\mathrm{M.C.M}(x, y)$. Por hipótesis, m verifica 1. y 2. por último, si ${}^{x}|_{r}$ e ${}^{y}|_{r}$, por el algoritmo de la división $r = mc + r'$ (demostrar que $r' = 0$). ■

Proposición 19 Sean x, y dos enteros no nulos. Entonces el mínimo común múltiplo de x e y es el producto de los primos comunes y no comunes elevado al mayor de los exponentes (en sus respectivas factorizaciones).

Corolario 20 (Ejercicio 8 (Pag. 48)) Sabemos que la relación de divisibilidad en $\mathbb{N}$ es una relación de orden. Además, el ínfimo de dos elementos $a, b \in \mathbb{N}$ coincide con $\mathrm{m.\,c.\,d}(a, b)$, y el supremo de dos elementos $a, b \in \mathbb{N}$ coincide con $\mathrm{M.\,C.\,M}(a, b)$, por lo que $\mathbb{N}$ con la relación de divisibilidad es un retículo.

Corolario 21 Sean x, y dos enteros no nulos. Entonces

$$|xy| = m.c.d(x, y).\,\mathrm{M.\,C.\,M}(x, y).$$

★ Los ejercicios del 7 al 21 de este tema pueden servirte para comprobar si has asimilado las nociones de estas dos secciones.

3. Congruencias.

3.1. Anillos de congruencias

En esta sección vamos a trabajar con nuevos conjuntos de números: $\mathbb{Z}_n$, los **anillos de congruencias modulo** n.

Definición 1 Sea $\mathbb{Z}$ el conjunto de los enteros y $n \in \mathbb{N}$. Dados $a, b \in \mathbb{Z}$, diremos que a es congruente con b módulo n, y lo representaremos por $a \equiv b \pmod n$ si ${}^{n}|_{a-b}$.

Proposición 2 Sea $\mathbb{Z}$ el conjunto de los enteros y $n \in \mathbb{N}$. Entonces:

(i) Para todo $a, b \in \mathbb{Z}$, $a \equiv b \pmod n$ si y sólo si el resto de dividir a por n coincide con el resto de dividir b por n.

(ii) La relación de congruencia es una relación de equivalencia,

(iii) Las clases de equivalencia de la relación de congruencia módulo n son

$$\mathbb{Z}_n := \mathbb{Z}/_{(\mathrm{mod}\, n)} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}.$$

Demo: (i). Aplicando el algoritmo de la división $a = cn + r$, $b = c'n + r'$. Podemos suponer que $r' \leq r$ (en caso contrario les cambiamos los nombres). Ahora, $a - b = (c - c')n + r - r'$ con $0 \leq r - r' \leq r < n$, por tanto $a - b$ es múltiplo de n si y sólo si $r - r' = 0$.

(ii). Trivial a partir de (i).

(iii). Dado $a \in \mathbb{Z}$, aplicando el algoritmo de la división, $a = cn + r$ con $0 \leq r < n$. Por tanto $a - r = cn$ y $a \equiv r \pmod n$ o lo que es lo mismo $\overline{a} = \overline{r}$ (hemos demostrado que a lo sumo hay n clases de equivalencia, $\{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$). Veamos ahora que todas son distintas: sean $0 \neq i \leq j < n$ y supongamos que $\overline{i} = \overline{j}$. Entonces $j \equiv i \pmod n$ por lo que $j - i = cn$. Por otro lado, $0 \leq j - i \leq j < n$, con lo que la única posibilidad es $j - i = 0n = 0$, es decir $i = j$ y hay n clases de equivalencia. ■

Nota: En el anillo de congruencias módulo n, con $n \in \mathbb{N}$, tenemos que la clase de equivalencia de un elemento $r \in \mathbb{Z}$ es:

$$\overline{r} = \{r + \alpha n \mid \alpha \in \mathbb{Z}\}$$

Es decir, cualquier elemento de este conjunto es un representante para la clase $\overline{r} \in \mathbb{Z}_n$.

Teorema 3 Sea $\mathbb{Z}$ el conjunto de los enteros y $n \in \mathbb{N}$. Entonces podemos definir una suma y un producto en el conjunto cociente, $\mathbb{Z}_n$:

(i) $\overline{a} + \overline{b} := \overline{a + b}$ para todo $\overline{a}, \overline{b} \in \mathbb{Z}_n$.

(ii) $\overline{a} \cdot \overline{b} := \overline{a \cdot b}$ para todo $\overline{a}, \overline{b} \in \mathbb{Z}_n$.

(iii) Las operaciones anteriores verifican las propiedades 1.(a),(b),(c),(d), 2.(a),(b),(c), 3.(a). de la definición 5 (Pag. 31).

Nota: No hay ninguna relación de orden asociada a este conjunto cociente. A $\mathbb{Z}_n$ con las operaciones anteriores se le denomina el **anillo de congruencias** módulo n. Observar que $\overline{0} = \{kn \mid k \in \mathbb{Z}\}$, es decir, los múltiplos de n son el elemento neutro de la suma.

Demo: En (i) y en (ii) se ha definido la suma y el producto respecto de representantes de cada clase, por lo que hay que demostrar que la suma y el producto están bien definidos (no dependen de representantes). Sean

$$\begin{array}{l} \overline{a} = \overline{a'} \\ \overline{b} = \overline{b'} \end{array} \implies \begin{array}{l} a - a' = cn \\ b - b' = c'n \end{array} \tag{1}$$

(i). Veamos que la suma está bien definida: por (1), sumando ambas expresiones, $a - a' + b - b' = (c + c')n$, o lo que es lo mismo,

$$a + b - (a' + b') = (c + c')n,$$

es decir, $a + b \equiv a' + b' \pmod{n}$ y por tanto $\overline{a + b} = \overline{a' + b'}$.

(ii). Veamos que el producto está bien definida: por (1), $a = a' + cn$ y $b = b' + c'n$ por tanto, si multiplicamos ambas expresiones,

$$ab = a'b' + a'c'n + b'cn + cc'n^2 = a'b' + (a'c' + b'c + cc'n)n.$$

Por tanto $ab \equiv a'b' \pmod{n}$ y por tanto $\overline{ab} = \overline{a'b'}$.

(iii). Todas estas propiedades son ahora triviales:

- Propiedades de la suma:
  - Asociativa: $\overline{x} + (\overline{y} + \overline{z}) = \overline{x} + \overline{y + z} = \overline{x + (y + z)} = \overline{(x + y) + z} = \overline{x + y} + \overline{z} = (\overline{x} + \overline{y}) + \overline{z}$.
  - Conmutativa: $\overline{x} + \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x}$.
  - Elemento neutro: $\overline{x} + \overline{0} = \overline{x + 0} = \overline{x}$.
  - Elemento opuesto: $\overline{x} + \overline{-x} = \overline{0}$.

- Propiedades del producto:
  - Asociativa: $\overline{x} \cdot (\overline{y} \cdot \overline{z}) = \overline{x} \cdot \overline{y \cdot z} = \overline{x \cdot (y \cdot z)} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot y} \cdot \overline{z} = (\overline{x} \cdot \overline{y}) \cdot \overline{z}$
  - Conmutativa: $\overline{x} \cdot \overline{y} = \overline{x \cdot y} = \overline{y \cdot x} = \overline{y} \cdot \overline{x}$.
  - Elemento Neutro: $\overline{x} \cdot \overline{1} = \overline{x \cdot 1} = \overline{x}$.
- Propiedades conjuntas (distributiva):

$$\overline{x} \cdot (\overline{y} + \overline{z}) = \overline{x} \cdot (\overline{y + z}) = \overline{x \cdot (y + z)} = \overline{x \cdot y + x \cdot z} = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z}.$$

Lo que demuestra la proposición. Se dice que $(\mathbb{Z}_n, +)$ es un grupo abeliano por cumplir las 4 primeras propiedades. Se dice que $(\mathbb{Z}_n, +, \cdot)$ es un anillo unitario por cumplir todas las propiedades anteriores. ■

Fin de clase 11; 21-10-2011, grupo A y B: Ejercicios. Fin de clase 12; 25-10-2011, grupo A y B

Corolario 4 *Sea $n \in \mathbb{N}$ y sean $a, b, c, d, x \in \mathbb{Z}$, $y \in \mathbb{N}$. Supongamos que $a \equiv b \pmod n$ y $c \equiv d \pmod n$. Entonces,*

(i) $a + c \equiv b + d \pmod n$ (ii) $a \cdot c \equiv b \cdot d \pmod n$.

(iii) $x \cdot a \equiv x \cdot b \pmod n$. (iv) $a^y \equiv b^y \pmod n$.

Nota: Se ha demostrado que si estamos trabajando en el anillo de congruencias modulo n cuando multiplicamos o sumamos número podemos cambiar cualquiera de ellos por un congruente (modulo n) suyo. Así, en $\mathbb{Z}_{11}$ tenemos:

$$(213 \cdot 543) + 1113 \equiv (4 \cdot 4) + 2 = 18 \equiv 7 \pmod{11}$$

En cambio no podemos cambiar por números congruentes las potencias (los exponentes nos dicen cuantas veces hay que multiplicar un elemento):

$$2^{12} \not\equiv 2^1 \pmod{11}$$

Ejemplos A Veamos las tablas de sumar y multiplicar de $\mathbb{Z}_6$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\bullet$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Nota: En estos conjuntos de números ocurren cosas extrañas: Por ejemplo, en $\mathbb{Z}_6$, $\overline{2}\,\overline{3} = \overline{0}$, por lo que el producto de números no nulos puede ser cero.

Definición 5 Sea $\mathbb{Z}_n$ el anillo de congruencias módulo n (con $n \in \mathbb{N}$). Diremos que $\overline{a} \in \mathbb{Z}_n$ **es inversible en** $\mathbb{Z}_n$ si existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1} = \overline{b} \cdot \overline{a}$

Proposición 6 Sea $\mathbb{Z}_n$ el anillo de congruencias módulo n (con $n \in \mathbb{N}$) y sea $\overline{a} \in \mathbb{Z}_n$. Entonces, $\overline{a}$ es inversible en $\mathbb{Z}_n$ si y solo si $\mathrm{m.\,c.\,d}(a, n) = 1$. Es más, en este caso, existe un único $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1} = \overline{b} \cdot \overline{a}$, llamado **el inverso de** $\overline{a}$ **en** $\mathbb{Z}_n$, que se denotará usualmente por $\overline{a}^{-1}$.

Demo: Supongamos que $\overline{a}$ es inversible en $\mathbb{Z}_n$, entonces existe $\overline{b} \in \mathbb{Z}_n$ tal que

$$\overline{a}\ \overline{b} = \overline{1}, \quad \text{es decir,} \quad ab \equiv 1 \pmod{n}$$

o lo que es lo mismo $ab - 1 = cn$. Por tanto, $ab + (-c)n = 1$, luego $\mathrm{m.\,c.\,d}(a, n) = d$ divide a 1, lo que implica $\mathrm{m.\,c.\,d}(a, n) = 1$. Por otro lado, si $\mathrm{m.\,c.\,d}(a, n) = 1$, aplicando el Teorema de Bezout existen $r, s \in \mathbb{Z}$ tales que $ar + cn = 1$ o lo que es lo mismo, $ar - 1 = -sn$, $(ar \equiv 1 \pmod{n})$ es decir, $\overline{a}\ \overline{r} = \overline{ar} = \overline{1}$.

Por último, si $\overline{b}, \overline{b}'$ son inversos para $\overline{a}$,

$$\overline{b} = \overline{b}\ \overline{1} = \overline{b}(\overline{a}\ \overline{b}') = (\overline{b}\ \overline{a})\overline{b}' = \overline{1}\ \overline{b}' = \overline{b}'.$$

Lo que demuestra la unicidad. ■

Corolario 7 Sea $\mathbb{Z}_n$ el anillo de congruencias módulo n (con $n \in \mathbb{N}$). Entonces, las siguientes condiciones son equivalentes:

(i) Todo elemento no nulo de $\mathbb{Z}_n$ es inversible.

(ii) n es un número primo.

(iii) Para todo par de elementos no nulos $\overline{a}, \overline{b}$ de $\mathbb{Z}_n$, $\overline{a}\ \overline{b} \neq \overline{0}$.

Demo: (ii) $\Longrightarrow$ (i). Por el resultado anterior, si n es primo, para todo $0 < k < n$, $\mathrm{m.\,c.\,d}(n, k) = 1$ y por tanto $\overline{k}$ es inversible en $\mathbb{Z}_n$.

(i) $\Longrightarrow$ (ii). Supongamos que todo elemento no nulo de $\mathbb{Z}_n$ es inversible. Entonces, para todo $k \in \mathbb{N}$, $0 < k < n$, se tiene que $\mathrm{m.\,c.\,d}(k, n) = 1$. Por tanto n no es divisible por ningún k tal que $0 < k < n$. Así, n es primo.

(i) $\Longrightarrow$ (iii). Sean $\overline{a}, \overline{b} \in \mathbb{Z}_n$ tales que $\overline{a}\ \overline{b} = \overline{0}$. Si $\overline{a} = \overline{0}$ no hay nada que demostrar, por tanto supongamos $\overline{a} \neq \overline{0}$. Entonces, $\overline{a}$ es inversible en $\mathbb{Z}_n$, sea $\overline{a}^{-1} \in \mathbb{Z}_n$ y por tanto,

$$\overline{0} = \overline{a}^{-1} \cdot \overline{0} = \overline{a}^{-1}(\overline{a}\ \overline{b}) = (\overline{a}^{-1}\ \overline{a})\overline{b} = \overline{1}\overline{b}$$

(iii) $\Longrightarrow$ (ii). Por reducción al absurdo, supongamos que n no es primo. Entonces existen $a, b \in \mathbb{Z}$, $1 < a, b < n$ tales que $n = ab$. Pero entonces $\overline{a}, \overline{b}$ son no nulos y $\overline{a}\ \overline{b} = \overline{n} = \overline{0}$, una contradicción. ■

Teorema 8 (Teorema de Fermat(chico)) *Sea $p, x \in \mathbb{N}$ con p un número primo y* $\mathrm{m.\,c.\,d}(p, x) = 1$. *Entonces* $x^{p-1} \equiv 1 \pmod{p}$.

Demo: Sea $\overline{x} \in \mathbb{Z}_p$. Como $\text{m. c. d}(p, x) = 1$, $\overline{x}$ es inversible en $\mathbb{Z}_p$, sea $\overline{y}$ su inverso. En estas condiciones tenemos que la aplicación $\Psi_x : \mathbb{Z}_p \to \mathbb{Z}_p$ definida por $\Psi_x(\overline{a}) = \overline{x}\ \overline{a}$ es inversible con inversa Ψ_y. Por tanto,

$$\mathbb{Z}_p = \text{Im}\,\Psi_x = \{\overline{x}\ \overline{1}, \overline{x}\ \overline{2}, \ldots, \overline{x}\ \overline{p-1}\}$$

Luego $\prod_{k=1}^{p-1} \overline{k} = \prod_{k=1}^{p-1} \overline{x}\ \overline{k} = \overline{x}^{p-1} \prod_{k=1}^{p-1} \overline{k}$. Por último, como $\prod_{k=1}^{p-1} \overline{k}$ es un elemento no nulo de $\mathbb{Z}_p$, multiplicando por su inverso, $\overline{x}^{p-1} = \overline{1}$ es decir, $x^{p-1} \equiv 1 \pmod p$. ■

Podemos encontrar una generalización de este teorema para cualquier número Natural, es el llamado Teorema de Euler:

Definición 9 Se define la **función de Euler** como $\varphi : \mathbb{N} \to \mathbb{N}$ definida por:

$$\varphi(n) = \#\{a \in \mathbb{N} \mid 1 \leq a \leq n,\ \text{m. c. d}(a, n) = 1\}$$

Por ejemplo, $\varphi(10) = 4$ o si p es un número primo, $\varphi(p) = p - 1$.

Proposición 10 $\varphi(n)$ coincide con el número de elementos inversibles en $\mathbb{Z}_n$

Proposición 11 (Ejercicio) Sea $\varphi : \mathbb{N} \to \mathbb{N}$ la función de Euler. Entonces

(i) Si p es un número primo y $r \in \mathbb{N}$, entonces $\varphi(p^r) = p^r(1 - \frac{1}{p}) = p^r - p^{r-1}$.

(ii) Si $n, m \in \mathbb{Z}$ con $\text{m. c. d}(n, m) = 1$, entonces $\varphi(nm) = \varphi(n)\varphi(m)$.

(iii) Si $n \in \mathbb{Z}$, $(n \neq 0, 1, -1)$ se factoriza como producto de primos $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, entonces

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$$

Teorema 12 (Teorema de Euler) *Sean $n, x \in \mathbb{N}$ con $\text{m. c. d}(n, x) = 1$. Entonces $x^{\varphi(n)} \equiv 1 \pmod n$.*

Demo: La demostración es muy similar a la demostración del teorema de Fermat. Consideremos Δ el conjunto de los elementos inversibles de $\mathbb{Z}_n$. Sea $\overline{x} \in \mathbb{Z}_n$. Como $\text{m. c. d}(n, x) = 1$, $\overline{x}$ es inversible en $\mathbb{Z}_p$, sea $\overline{y}$ su inverso. En estas condiciones tenemos que la aplicación $\Psi_x : \Delta \to \Delta$ definida por $\Psi_x(\overline{a}) = \overline{x}\ \overline{a}$, está bien definida, y es inversible con inversa Ψ_y. Por tanto,

$$\Delta = \text{Im}\,\Psi_x = \{\overline{x}\ \overline{a} \mid \overline{a} \in \Delta\}$$

Luego $\prod_{a\in\Delta} \overline{a} = \prod_{a\in\Delta} \overline{x}\ \overline{a} = \overline{x}^{\varphi(n)} \prod_{a\in\Delta} \overline{a}$. Por último, como $\prod_{a\in\Delta} \overline{a}$ es un elemento inversible de $\mathbb{Z}_p$, multiplicando por su inverso, $\overline{x}^{\varphi(n)} = \overline{1}$ o lo que es lo mismo, $x^{\varphi(n)} \equiv 1 \pmod n$. ■

Fin de clase 13; 28-10-2011, grupo A y B (clase día 27 se recuperará. Martes 1 Fiesta. Jueves y viernes en congreso en Zaragoza. Recuperar 3 dias)

3.2. Sistemas de ecuaciones en congruencias

Ejemplos B Estudiemos ahora ecuaciones en los anillos de congruencias $\mathbb{Z}_n$. Supongamos que queremos encontrar las soluciones de la ecuación

$$\overline{3}\overline{x} = \overline{5} \quad \text{en } \mathbb{Z}_6. \tag{1}$$

o lo que es lo mismo, $3x \equiv 5 \pmod 6$. En estos momentos la única posibilidad que tenemos es comprobar, sustituyendo, si tiene o no tiene soluciones:

$$\begin{aligned} &3\cdot 0 \equiv 0 \pmod 6, \quad 3\cdot 1 \equiv 3 \pmod 6, \quad 3\cdot 2 \equiv 0 \pmod 6,\\ &3\cdot 3 \equiv 3 \pmod 6, \quad 3\cdot 4 \equiv 0 \pmod 6, \quad 3\cdot 5 \equiv 3 \pmod 6 \end{aligned}$$

luego no tiene soluciones. Sin embargo, la ecuación

$$\overline{6}x = \overline{4} \quad \text{en } \mathbb{Z}_8. \tag{2}$$

tiene por soluciones $x = 2$ y $x = 6$:

$$\begin{aligned} &6\cdot 0 \equiv 0 \pmod 8, \quad 6\cdot 1 \equiv 6 \pmod 8, \quad 6\cdot 2 \equiv 4 \pmod 8,\\ &6\cdot 3 \equiv 2 \pmod 8, \quad 6\cdot 4 \equiv 0 \pmod 8, \quad 6\cdot 5 \equiv 6 \pmod 8,\\ &6\cdot 6 \equiv 4 \pmod 8, \quad 6\cdot 7 \equiv 2 \pmod 8, \end{aligned}$$

Nota: Observar que, "simplificando" la ecuación anterior por 2, $\overline{3}x = \overline{2}$, tiene una única solución $x = 6$ (luego $x = 2$ ha dejado de ser solución!!).

Proposición 13 Sean $n_1, n_2, \ldots, n_k, r, s, u, v, n, m \in \mathbb{Z}$ elementos no nulos.

(i) Supongamos que para cada $i \in \{1, 2, \ldots, k\}$, $\text{m. c. d}(s, n_i) = 1$ y sea $m = \prod_{i=1}^{k} n_i$. Entonces $\text{m. c. d}(s, m) = 1$.

(ii) Si s divide a uv, y $\text{m. c. d}(s, u) = 1$, entonces s divide a v.

(iii) Si ${}^{n}|_{s}$ y ${}^{m}|_{s}$ con $\text{m. c. d}(n, m) = 1$, entonces ${}^{nm}|s$

(iv) Si $\text{m. c. d}(n, m) = d$, y sean n' y m' tales que $n = n'd$ y $m = m'd$. Entonces $\text{m. c. d}(n', m') = 1$.

Demo: (i) Sea $d = \text{m. c. d}(s, m)$. Por reducción al absurdo, supongamos que $d > 1$. Entonces podemos factorizar d como producto de primos. Sea p uno de los primos que aparece en la factorización de d. Tenemos entonces que d divide a s y de divide a $m = \prod_{i=1}^{k} n_i$. Luego por la proposición 14 (Pag. 37) existe un k tal que p divide a n_k (si un primo p divide a un producto de números, entonces divide a alguno de ellos). Pero entonces (${}^{p}|_{s}$ y ${}^{p}|_{n_k}$), p divide a $\text{m. c. d}(s, n_k) = 1$, una contradicción. Por tanto $d = 1$.

(ii) Si $\text{m. c. d}(s, u) = 1$ y $vu = \gamma s$, por Bezout existen $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha s + \beta u = 1$. Si multiplicamos ahora por v,

$$v = \alpha s v + \beta u v = \alpha s v + \gamma s = (\alpha v + \gamma)s$$

Lo que demuestra que s divide a v.

(iii) Por hipótesis $s = \alpha m$ y $s = \beta n$. Aplicando el Teorema de Bezout, existen $x, y \in \mathbb{Z}$ tales que $xn + ym = 1$. Por tanto, multiplicando esta igualdad por s obtenemos

$$s = sxn + sym = \alpha mxn + \beta nym = (\alpha x + \beta y)nm$$

Por tanto s es divisible por nm.

(iv) Por el teorema de existencia del máximo común divisor, existen $r, s \in \mathbb{Z}$ tales que

$$d = rn + sm = rn'd + sm'd = (rn' + sm')d.$$

Aplicando ahora la ley de simplificación en $\mathbb{Z}$ tenemos que $rn' + sm' = 1$, por lo que por el Teorema de Bezout, $\text{m. c. d}(n'.m') = 1$. ■

Nota: Podemos pensar en una ecuación $\overline{a} \cdot x = \overline{b}$ en $\mathbb{Z}_n$, el anillo de congruencias módulo n, con $n \in \mathbb{N}$, o podemos pensar en la ecuación en congruencias $ax \equiv b \pmod n$. En ambos casos se trata del mismo problema, en el primero las soluciones serán elementos de $\mathbb{Z}_n$ (con lo que con dar un representante de cada solución es suficiente. En el segundo tenemos que dar todos los elementos de $\mathbb{Z}$ que verifican la ecuación, que no es más que cualquier representante de las soluciones en $\mathbb{Z}_n$: Así,

- La ecuación $\overline{3} \cdot x = \overline{4}$ en $\mathbb{Z}_5$ tiene por solución $x = \overline{3} \in \mathbb{Z}_5$.
- La ecuación $3x \equiv 4 \pmod 5$ tiene por solución el conjunto

$$S = \{\cdots, -12, -7, -2, 3, 8, 13, \cdots\}.$$

Que no es más que el conjunto definido por $\overline{3}$.

Trabajaremos indistintamente con una ecuación que con otra. Cuando se hable sobre el numeró de soluciones de alguna de estas ecuaciones nos estaremos refiriendo al número de soluciones en $\mathbb{Z}_n$ (ya que en $\mathbb{Z}$ o no tiene soluciones o son infinitas)

Teorema 14 Sean $n \in \mathbb{N}$ y $a, b \in \mathbb{Z}$. Entonces las siguientes condiciones son equivalentes:

(i) La ecuación $ax \equiv b \pmod n$ tiene solución.

(ii) El máximo común divisor de a y n divide a b.

Además, el número de soluciones de la ecuación (en $\mathbb{Z}_n$) es exactamente el $\text{m. c. d}(a, n)$.

Demo: Denotemos por $d = \text{m. c. d}(a, n)$. Supongamos que $s \in \mathbb{Z}$ es solución de la ecuación

$$ax \equiv b \pmod n.$$

Entonces existe $\alpha \in \mathbb{Z}$ tal que $as - b = \alpha n$. Por tanto $b = as - \alpha n$. Ahora, como a y n son divisibles por d (esto es por definición), b es divisible por d.

Supongamos ahora que b es divisible por d, $b = \beta d$. Por el Teorema 7 (Pag. 34) existen $r, s \in \mathbb{Z}$ tales que $d = ra + sn$. Si multiplicamos por β en esta igualdad obtenemos que $b = \beta d = \beta(ra + sn)$, lo que implica que $\beta ra - b = \beta sn$, o lo que es lo mismo, $a(\beta r) \equiv b \pmod n$, es decir, βr es solución de la ecuación.

Demostremos ahora el además: Supongamos que la ecuación $ax \equiv b \pmod n$ tiene solución, sea s una solución de la ecuación. Por lo anterior sabemos que $d = \text{m. c. d}(a, n)$ divide a b. Sean $\alpha, \gamma \in \mathbb{Z}$ tales que $n = \gamma d$, $a = \alpha d$. Veamos que $s + \gamma$ es también solución de la ecuación.

$$a(s + \gamma) = as + a\gamma \equiv b + a\gamma = b + \alpha d\gamma = b + \alpha n \equiv b \pmod n$$

Luego para todo $k \in \mathbb{N}$, $s + k\gamma$ es solución. Como nos estamos preocupando de las soluciones módulo n, la solución $s + d\gamma = s + n \equiv s \pmod{n}$ por lo que k toma los valores $0 \leq k \leq d - 1$. Por tanto, como mucho tenemos las siguientes d soluciones

$$\{s, s + \gamma, s + 2\gamma, \ldots, s + (d - 1)\gamma\}$$

Observar que todas son distintas, módulo n, ya que si

$$0 \leq t_1 < t_2 \leq d - 1 \text{ y } s + t_1\gamma \equiv s + t_2\gamma \pmod{N},$$

entonces $0 \leq (t_2 - t_1)\gamma \leq t_2\gamma < d\gamma = n$ y por tanto como $(t_2 - t_1)\gamma = \dot{n}$ (es múltiplo de n) éste tiene que ser cero, una contradicción, $t_1 = t_2$.

Por último, si s' es solución del sistema, $a(s'-s) \equiv 0 \pmod{n}$ y por tanto $a(s'-s) = \tau n$ dividiendo en esta igualdad por d obtenemos

$$d\alpha(s' - s) = a(s' - s) = \tau n = \tau\gamma d$$

por lo que $\alpha(s' - s) = \tau\gamma$ y como $\text{m. c. d}(\alpha, \gamma) = 1$, por la proposición anterior, γ divide a $s' - s$ por lo que $s' - s = \xi\gamma$ y por tanto $s' = s + \xi\gamma$ es una de las soluciones anteriores. ■

El siguiente resultado nos va a permitir calcular más fácilmente las soluciones de una ecuación en congruencias cuando el número de soluciones (En $\mathbb{Z}_n$) es mayor que 1:

Proposición 15 (Ejercicio) *Sean $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$. Supongamos que $1 < \text{m. c. d}(a, n) = d$ y que d divide a b. Tenemos entonces que $a = da'$, $n = dn'$ y $b = db'$. Entonces el conjunto de soluciones en $\mathbb{Z}$ de las siguientes ecuaciones coincide*

$$ax \equiv b \pmod{n} \qquad a'x \equiv b' \pmod{n'}$$

Demo: Sea $s \in \mathbb{Z}$ una solución de $ax \equiv b \pmod{n}$. Entonces $as - b = \dot{n}$, por lo que existe $\alpha \in \mathbb{Z}$ tal que $as - b = \alpha n$. Es decir, $a'dx - db' = \alpha dn'$. Si simplificamos ahora por d tenemos que $a'x - b' = \alpha n'$, lo que demuestra que s es solución de la ecuación $a'x \equiv b' \pmod{n'}$.

Sea $s \in \mathbb{Z}$ una solución de $a'x \equiv b' \pmod{n'}$. Entonces existe $\beta \in \mathbb{Z}$ tal que $a's - b' = \beta n'$. Si multiplicamos ahora esta igualdad por d tenemos, $a'dx - db' = \alpha dn'$. Es decir, $as - b = \beta n$, lo que demuestra que s es solución de la ecuación $ax \equiv b \pmod{n}$. ■

Nota: La proposición anterior es muy útil a la hora de resolver ecuaciones en congruencias: Resuelve la ecuación en congruencias

$$4x \equiv 4 \pmod{8}$$

Como $\text{m. c. d}(4, 8) = 4$ y 4 divide a 4, esta ecuación tiene solución, es más, modulo 8 el número de soluciones es 4. Por la proposición anterior, esta ecuación tiene las mismas soluciones en $\mathbb{Z}$ que la ecuación

$$x \equiv 1 \pmod{2}$$

que claramente es el conjunto

$$\{1 + 2k, \quad k \in \mathbb{Z}\}.$$

Por tanto las soluciones distintas en $\mathbb{Z}_8$ son $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ ($\overline{9}$ ya coincide con $\overline{1}$ en $\mathbb{Z}_8$).

Fin de clase 14; 8-11-2011, grupo A y B

Teorema 16 Sean $n_1, n_2, \ldots, n_k \in \mathbb{N}$ y $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. Supongamos que m. c. d$(n_i, n_j) = 1$ para todo $i, j \in \{1, 2, \ldots, k\}$, $i \neq j$. Entonces el sistema de ecuaciones:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Tiene solución. Es más, ésta es única modulo $m = \prod_{i=1}^{k} n_i$.

Demo: Vamos a dar una demostración constructiva, lo que nos servirá para resolver casos concretos. Construimos k y resolvemos k ecuaciones en congruencias independientes: sean $m_i = m/n_i$ y consideremos las ecuaciones (independientes)

$$m_i x \equiv a_i \pmod{n_i} \qquad \text{para,} \quad i = \{1, 2, \ldots, k\}$$

Sea s_r solución de la ecuación r-esima ecuación, $m_r x \equiv a_r \pmod{n_r}$. Veamos que $s = \sum_{i=1}^{k} m_i s_i$ es solución de nuestro sistema.

$$s = \sum_{i=1}^{k} m_i s_i \equiv m_r s_r \equiv a_r \pmod{n_r} \quad \text{para todo } r \in \{1, 2, \ldots, k\}$$

Supongamos ahora que s y s' son soluciones del sistema. Entonces como $s \equiv a_i \pmod{n_i}$ y $s' \equiv a_i \pmod{n_i}$,

$$s - s' \equiv 0 \pmod{n_i}. \tag{1}$$

Por último, veamos, aplicando un proceso de inducción, que $s - s'$ es divisible por m: si $k = 1$ no tenemos nada que demostrar, por (1), $s - s'$ es divisible por n_1. Supongamos que el resultado es cierto para $k - 1$ y demostrémoslo para k: por hipótesis $s - s'$ es divisible por $\prod_{1=1}^{k-1} n_i$ y por (1) $s - s'$ es divisible por n_k. Luego como m. c. d$(\prod_{1=1}^{k-1} n_i, n_k) = 1$, por la proposición anterior, $s - s'$ es divisible por $(\prod_{1=1}^{k-1} n_i) n_k = m$, lo que demuestra el teorema. ■

★ Los ejercicios del 22 al 39 de este tema pueden servirte para comprobar si has asimilado las nociones de esta sección.

4. Ejercicios de Tema

1 Demuestra que para todo $n \in \mathbb{N}$, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

2 Encuentra un modelo que verifique los 4 primeros axiomas de Peano pero no el principio de inducción matemática. *

3 Encuentra un modelo que verifique los axiomas 1,2,4,5 de Peano. *

4 Encuentra un modelo que verifique los axiomas 1,2,3,5 de Peano. *

5 Sean $x, y \in \mathbb{N} \cup \{0\}$. Demuestra que si x es múltiplo de y y $x < y$, entonces $x = 0$

6 Demuestra que 1 solo es divisible por 1 y -1.

7 *Sean $x, y, a, b \in \mathbb{Z}$, Entonces:*

(i) Si ${}^{x}|_{y}$, entonces $\mathrm{m.c.d}(x, y) = |x|$.

(ii) Si ${}^{x}|_{a}$ y ${}^{x}|_{b}$, entonces ${}^{x}|_{\alpha a+\beta b}$ para todo $\alpha, \beta \in \mathbb{Z}$.

8 Demuestra que la relación de divisibilidad es reflexiva, transitiva y verifica que para todo $a, b \in \mathbb{Z}$,

$$ {}^{a}|_{b} \text{ y } {}^{b}|_{a} \quad \text{entonces } a = \pm b. $$

Por tanto es una relación de orden en $\mathbb{N}$. ¿Quien es el supremo y el ínfimo de dos elementos $a, b \in \mathbb{N}$?

9 Demuestra que el máximo común divisor de dos enteros no nulos $x, y \in \mathbb{Z}$. coincide con el producto de los primos comunes elevados al menor exponente.

10 Sean $p_1, p_2, \cdots, p_k$ números primos. Demuestra que en la factorización de $p_1 \cdots p_k + 1$ no aparece ninguno de los primos anteriores.

11 Sean $0 \neq a, b \in \mathbb{Z}$ tales que $3a + 8b = 2$. Entonces $\mathrm{m.c.d}(b, 3) = 1$.

12 Demuestra los siguientes criterios de divisibilidad:

- x es divisible por 2 si y sólo si su última cifra es divisible por 2.
- x es divisible por 8 si y sólo si sus tres últimas cifras son divisibles por 8.
- x es divisible por 3 si y sólo si la suma de sus cifras es divisible por 3.
- x es divisible por 11 si y sólo si la suma de sus cifras en posición par menos la suma de sus cifras en posición impar es divisible por 11.

13 El algoritmo de la división dice que dados $x, y \in \mathbb{Z}$ con $y > 0$ existen unos únicos $c, r \in \mathbb{Z}$ con $0 \leq r < y$ tales que $x = cy + r$. Demuestra que el resultado también es cierto si $y < 0$, es decir: Demuestra que dados $x, y \in \mathbb{Z}$ con $y \neq 0$ existen unos únicos $c, r \in \mathbb{Z}$ con $0 \leq r < |y|$ tales que $x = cy + r$.

14 Sean a, b dos elementos no nulos de $\mathbb{Z}$ y sean $s, r \in \mathbb{Z}$ tales que $sa + rb = \text{m. c. d}(a, b)$. Demuestra que r y s son primos relativos. $\boxed{*}$

15 Sean $x, y, r, s \in \mathbb{Z}$ no nulos tales que $rx + sy = 1$. Demuestra que

$$\text{m. c. d}(x, y) = \text{m. c. d}(x, s) = \text{m. c. d}(r, y) = \text{m. c. d}(r, s) = 1.$$

¿Que se puede decir del $\text{m. c. d}(r, x)$?

16 Sean $n, m, s \in \mathbb{Z}$ no nulos tales que $\text{m. c. d}(n, s) = 1$. Supongamos que s divide al producto $n \cdot m$. Demuestra entonces que s divide a m. ¿Es cierto el resultado si s y n no son primos relativos?

17 (Teorema Generalizado de Bezout) Sean $n_1, n_2, \ldots, n_k \in \mathbb{N}$ tales que si $k \in \mathbb{N}$ divide a todo n_i, entonces $k = 1$. Demuestra que existen $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}$ tales que $\alpha_1 n_1 + \alpha_2 n_2 + \cdots + \alpha_k n_k = 1$. $\boxed{**}$

18 Sean $n_1, n_2, \ldots, n_k, s \in \mathbb{Z}$ elementos no nulos. Supongamos que para cada $i \in \{1, \ldots, k\}$, $\text{m. c. d}(s, n_i) = 1$. Demuestra $\text{m. c. d}(s, \prod_{i=1}^{k} n_i) = 1$.

19 Demuestra que existe el mínimo común múltiplo de dos elementos no nulos $x, y \in \mathbb{Z}$ y que éste es único. $\boxed{*}$

20 Sean n, m dos elementos no nulos de $\mathbb{Z}$. Demuestra que

$$\text{m. c. d}(n, m).\,\text{M. C. M}(n, m) = |n \cdot m|.$$

21 Sean $a, b \in \mathbb{Z}$. Demuestra que nunca puede suceder que $6a + 21b = \text{m. c. d}(a, b)$. $\boxed{*}$

22 Sea $n \in \mathbb{N}$ y $a, b \in \mathbb{Z}$. Demuestra que la ecuación $ax \equiv b \pmod{n}$ tiene una única solución si y sólo si $\text{m. c. d}(a, n) = 1$. $\boxed{*}$

23 Calcula el resto de dividir 11^{1151} entre 7 y de dividir 13^{1111} entre 15.

24 Si es martes y trece y la luna está llena, ¿Cuantos dias habrá que esperar para que sea viernes con luna nueva? (ciclo lunar 30 dias) $\boxed{*}$

25 Demuestra que en $\mathbb{Z}_n$ no de da la ley de simplificación: Existen a, b, c elementos no nulos de $\mathbb{Z}_n$ (para algún n) tal que

$$\overline{a}\,\overline{b} = \overline{a}\,\overline{c} \quad \text{y} \quad \overline{b} \neq \overline{c}$$

26 Sea $\varphi : \mathbb{N} \to \mathbb{N}$ la función de Euler. Entonces $\boxed{***}$

(i) Si p es un número primo y $r \in \mathbb{N}$, entonces $\varphi(p^r) = p^r(1 - \frac{1}{p}) = p^r - p^{r-1}$.

(ii) Si $n, m \in \mathbb{Z}$ con $\text{m. c. d}(n, m) = 1$, entonces $\varphi(nm) = \varphi(n)\varphi(m)$.

(iii) Si $n \in \mathbb{Z}$, $(n \neq 0, 1, -1)$ se factoriza como producto de primos $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, entonces

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$$

27 Resuelve el siguiente sistema de ecuaciones en congruencias:

$$\begin{cases} 4x \equiv 5 \pmod 9 \\ 5x \equiv 2 \pmod{24} \end{cases}$$

28 Resuelve el siguiente sistema de ecuaciones en congruencias:

$$\begin{cases} 2x \equiv 3 \pmod 5 \\ 3x \equiv 5 \pmod{13} \end{cases}$$

29 Calcula las dos últimas cifras del número 21^{3553}.

30 Calcula las soluciones de los siguientes sistemas (caso de que tengan):

(a). $2x \equiv 3 \pmod 5$ (b). $15x \equiv 3 \pmod 6$ (c). $21x \equiv 14 \pmod{35}$
(d). $4x \equiv 10 \pmod 8$ (e). $6x \equiv 6 \pmod{12}$ (f). $x^2 \equiv 3 \pmod 7$

31 ¿Las ecuaciones $\overline{9} \cdot x = \overline{15}$, $\overline{3} \cdot x = \overline{5}$ y $\overline{6} \cdot x = \overline{10}$ tienen las mismas soluciones en $\mathbb{Z}_{12}$? ¿Explica la razón?

32 Sea $n \in \mathbb{N}$ y sea $\overline{z} \in \mathbb{Z}_n$ con $\mathrm{m.c.d}(z, n) = 1$. Demuestra que las ecuaciones

$$a \cdot X \equiv b \pmod n \quad \text{y} \quad za \cdot X \equiv zb \pmod n$$

tienen las mismas soluciones.

33 Sea $n \in \mathbb{N}$ sea $\overline{a} \in \mathbb{Z}_n$. Se dice que un elemento $0 \neq \overline{b} \in \mathbb{Z}_n$ es un divisor de cero de $\overline{a}$ si $\overline{a} \cdot \overline{b} = \overline{0}$. Demuestra que el número de divisores de cero de $\overline{a}$ en $\mathbb{Z}_n$ coincide con $\mathrm{m.c.d}(a, n) - 1$. $\boxed{*}$

34 Resuelve los siguientes sistemas de ecuaciones en congruencias:

$$\begin{cases} 2x \equiv 3 \pmod 6 \\ 3x \equiv 5 \pmod 9 \end{cases} \qquad \begin{cases} 2x \equiv 2 \pmod 6 \\ 3x \equiv 6 \pmod 9 \end{cases} \qquad \begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}$$

35 Resuelve los siguientes sistemas de ecuaciones en congruencias:

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$$

36 Calcula todas las soluciones de la ecuación $x^6 \equiv 1 \pmod 7$. Explica el resultado.

37 Sean $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$. Supongamos que $1 < \mathrm{m.c.d}(a, n) = d$ y que d divide a b. Tenemos entonces que $a = da'$, $n = dn'$ y $b = db'$. Entonces el conjunto de soluciones en $\mathbb{Z}$ de las siguientes ecuaciones coincide

$$ax \equiv b \pmod n \qquad a'x \equiv b' \pmod{n'}$$

38 Una pecera es limpiada cada 29 dias y a los peces se les dá de comer cada 4. Si hace 3 dias que han comido y 15 que se les ha limpiado la pecera, ¿Cuantos días tienen que esperar los peces para que se les limpie y coman el mismo día?

39 Sabemos que $\overline{40} = \overline{74} = -\overline{45}$ en $\mathbb{Z}_n$ ¿Quien puede ser n?

40 ¿Es un conjunto la colección de los números naturales que se pueden describir con menos de 15 palabras en castellano? $\boxed{***}$

Capítulo 3

Anillos

Objetivos del capítulo

- Se recuerda el concepto abstracto de relación binaria. Se estudian las propiedades asociadas a una relación binaria. Se pretende que propiedades que han sido estudiadas en diferentes momentos se asimilen como un mismo concepto (unicidad del inverso en aplicaciones biyectivas o en $\mathbb{Z}_n$).
- Se introduce la noción abstracta de Anillo y sus propiedades. Se estudian los elementos inversibles de un anillo introduciendo la noción de anillos de división y cuerpo.
- Se empiezan a estudiar métodos para encontrar Anillos nuevos a partir de anillos dados: se estudian subanillos, la suma y el producto directo de anillos, los anillos de matrices, de polinomios y de series formales. Se estudian el anillos de endomorfismos de un grupo abeliano.
- Se estudian las aplicaciones naturales entre anillos, los homomorfismos de anillos y sus propiedades.
- Se estudia la unitización y la característica de un anillo.

---

1. Operación binaria, semigrupo, monoide.

Definición 1 Sea X un conjunto no vacío. Se define una **operación binaria** en X como una aplicación $* : X \times X \to X$. Normalmente, un conjunto con una operación binaria se denotará por $(X, *)$.

Nota: Genéricamente dados $a, b \in X$ denotaremos al producto de a con b como $a * b$ y se leerá a operado con b. En casos concretos nos van a aparecer dos notaciones distinta de producto (de hecho, ya estamos acostumbrados a ellas):

- La notación multiplicativa, $a * b$, $a \cdot b$ o simplemente ab (la operación simplemente se denota por yuxtaposición)
- La notación aditiva, $a + b$ (la operación se denota por "+").

Ejemplos A

$\star$ La suma o el producto en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$ o $\mathbb{R}$.

⋆ La resta en $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$ (la resta no es operación en $\mathbb{N}$).

⋆ La división no es operación binaria en ninguno de estos conjuntos.

⋆ La división es una operación binaria en $\mathbb{Q} - \{0\}$ o $\mathbb{R} - \{0\}$.

⋆ El máximo común divisor y el mínimo común múltiplo son operaciones binarias en $\mathbb{Z}$.

⋆ La unión, la intersección, la diferencia o la diferencia simétrica son operaciones binarias.

⋆ La composición de aplicaciones es una operación binaria en $\Delta := \{f \mid f : X \to X\}$.

⋆ Dado un conjunto no vacío X, las siguientes son operaciones binarias en X: dado $c \in X$, para todo $a, b \in X$ definimos,

$$\begin{aligned} a * b &= a \\ a * b &= b \\ a * b &= c \end{aligned}$$

Definición 2 Sea X un conjunto no vacio y $*$ una operación en X. Se dice que $*$

- es **asociativa** si $\forall\ a, b, c \in X, \quad a * (b * c) = (a * b) * c$.
- es **conmutativa** si $\forall\ a, b \in X, \quad a * b = b * a$.
- Posee elemento **neutro por la derecha** si existe $e \in X$ tal que $\forall\ a \in X$, $a * e = a$.
- Posee elemento **neutro por la izquierda** si existe $e \in X$ tal que $\forall\ a \in X$, $e * a = a$.
- Posee elemento neutro si existe elemento **neutro** por la izquierda y por la derecha.

Lema 3 Si e es neutro por la izquierda y e' es neutro por la derecha, entonces $e = e'$. Por lo que el elemento neutro, caso de existir es único.

$$e' = e * e' = e.$$

e es neutro por la izquierda

e' es neutro por la derecha

Corolario 4 Sea X un conjunto no vacío y $*$ una operación en X. Entonces, si $*$ posee elemento neutro éste es único.

Demo: Corolario trivial de lo anterior. ■

Nota: Sea X un conjunto con una operación que posee elemento neutro. Dependiendo de que notación estemos usando para denotar dicha operación así denotaremos al elemento neutro:

- En notación multiplicativa (la operación se denota por $*$, $\cdot$ o por yuxtaposición): al elemento neutro se le suele denotar por e o a veces por 1.
- En notación aditiva (la operación se denota por $+$): al elemento neutro se le suele denotar por 0.

Definición 5 Sea X un conjunto no vacío y $*$ una operación en X.

- Diremos que $(X, *)$ es un **semigrupo** si $*$ es asociativa.

• Diremos que $(X, *)$ es un **monoide** si $*$ es asociativa con elemento unidad (normalmente denotado por e, si la notación es multiplicativa, a veces, por 1 y si es aditiva, por 0).

• Un monoide $(X, *)$ con operación $*$ conmutativa se dirá **monoide conmutativo**.

Nota: Tal como su nombre indica, en una operación binaria podemos operar elementos de dos en dos. Por tanto, en principio, no tiene sentido expresiones tales como $a * b * c$. No obstante, si $*$ es asociativa tenemos que $(a * b) * c = a * (b * c)$. El siguiente teorema demuestra que es innecesario el uso de paréntesis en una operación asociativa.

Fin de clase 15; 10-11-2011, grupo A y B

Teorema 6 Sea $(X, *)$ un semigrupo. Entonces el producto arbitrario de n elementos de X es independiente de la disposición de los paréntesis.

Demo: Por hipótesis

$$(a * b) * c = a * (b * c)$$

por lo que lo podremos denotar por $a * b * c$.

$$(((a * b) * c) * d) = (a * b) * (c * d) = (a * (b * (c * d)))$$

se denotará por $a * b * c * d$. Supongamos que en un producto de $n-1$ elementos no afecta la posición de los paréntesis y consideremos un producto de n términos. Entonces:

♦ Los paréntesis del último producto serán $(a_1 * \cdots * a_k) * (a_{k+1} * \cdots * a_n)$ para algún $k \in \{1, \ldots, n-1\}$. Por la hipótesis de inducción los paréntesis interiores a éstos pueden ordenarse como mejor nos convenga. Por último, al ser la operación asociativa:

$$(a_1 * \cdots * a_k) * (a_{k+1} * (a_{k+1} * \cdots * a_n)) = (a_1 * \cdots * a_{k+1}) * (a_{k+2} * \cdots * a_n)$$
$$((a_1 * \cdots * a_{k-1}) * a_k) * (a_{k+1} * \cdots * a_n) = (a_1 * \cdots * a_{k-1}) * (a_k * \cdots * a_n)$$

Por lo que el último producto, y por tanto todos, pueden ser cambiados a nuestro antojo. Lo que demuestra el teorema. ■

Nota: Observar que aquí teníamos que demostrar que una propiedad era cierta para todo natural mayor que 3 y hemos adaptado el principio de inducción generalizado a este caso.

Definición 7 Sea $(M, *)$ un monoide con elemento unidad e. Diremos que un elemento $a \in X$ posee

- **Inverso por la izquierda** si existe $b \in X$ tal que $b * a = e$.
- **Inverso por la derecha** si existe $b \in X$ tal que $a * b = e$.
- **Inverso** si existe $b \in X$ tal que $a * b = e = b * a$.

Ejemplos B *Sea X un conjunto no vacio y sea $M = \{f : X \to X\}$, el conjunto de todas las aplicaciones de X en X. Tenemos entonces que $(M, \circ)$ es un monoide unitario ($\circ$ es la composición de aplicaciones, por lo que esta operación es asociativa y el elemento neutro es la aplicación identidad). Entonces, el apartado (i) de la proposición 11 (Pag. 12) nos dice que un elemento $f \in M$ posee inversa por la derecha si y sólo si f es una aplicación sobreyectiva y el apartado (ii) de la proposición 11 (Pag. 12) nos dice que un elemento $f \in M$ posee inversa por la izquierda si y sólo si f es una aplicación inyectiva.*

Lema 8 Sea $(M, *)$ un monoide con elemento neutro e y sea $a \in M$. Entonces:

(i) Si a tiene un inverso por la izquierda y un inverso por la derecha, ambos coinciden y a es inversible.

(ii) Si a posee inverso éste es único. Por tanto lo denotaremos de forma especial. Así, el inverso de un elemento $a \in M$ se denotará por:

- a^{-1} si estamos en notación multiplicativa.
- $-a$ si estamos en notación aditiva.

Demo: Sea b inverso por la izquierda de a y b' inversos por la derecha de a. Tenemos entonces que

$$b' = e * b' = (b * a) * b' = b * (a * b') = b * e = b. \qquad \blacksquare$$

Nota: El inverso de un elemento no tiene porqué existir: por ejemplo en $(\mathbb{Z}_6, \cdot)$ ($\mathbb{Z}_6$ con el producto) $\overline{3}$ no tiene inverso [no hay ningún elemento de $\mathbb{Z}_6$ que cuando lo multiplico por $\overline{3}$ me de $\overline{1}$]. En $\mathbb{Z}$ con el producto no suele haber inversos (solo el 1 y el -1 tienen inversos). Por tanto, aunque sea muy grande la tentación (por ejemplo para resolver un ejercicio) si $a \in G$ (G un conjunto con una operación) no puede aparecer de improviso el elemento a^{-1} a no ser que demostremos que a posee inverso, en particular G tiene que ser un monoide.

Nota: Ya hemos estudiado muchos elementos inversible en este curso: Los opuestos para la suma en $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ó $\mathbb{Z}_n$ verifican esta propiedad. Los inversos en $\mathbb{R}, \mathbb{Q}, \mathbb{Z}_n$ o las aplicaciones inversibles verifican esta propiedad.

Definición 9 Sea $(M, *)$ un monoide. Se dice que un elemento $a \in M$ es una **unidad de** M, si es un elemento inversible de M. El conjunto de las unidades de un monoide M se denota por $\mathcal{U}(M)$.

Proposición 10 Sea $(M, *)$ un monoide y sean $a, b \in M$. Entonces:

(i) El elemento neutro de M es una unidad.

(ii) Si a es una unidad, a^{-1} es una unidad y $(a^{-1})^{-1} = a$.

(iii) Si a y b son unidades de M, $a * b$ es una unidad de M y $(a * b)^{-1} = b^{-1} * a^{-1}$.

(iv) En general el producto arbitrario de unidades es una unidad.

$$(a_1 * \cdots * a_{n-1} * a_n)^{-1} = a_n^{-1} * a_{n-1}^{-1} * \cdots * a_1^{-1}$$

Demo: (i) y (ii) son triviales.

(iii) Veamos que $b^{-1} * a^{-1}$ es el inverso de $a * b$:

$$\begin{aligned} (a * b) * (b^{-1} * a^{-1}) &= a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e \\ (b^{-1} * a^{-1}) * (a * b) &= b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = e \end{aligned}$$

(iv) Vamos a dar una demostración por inducción: el caso $n = 2$ es el apartado anterior. Supongamos que el resultado es cierto para $n - 1$, entonces:

$$\begin{aligned} (a_1 * \cdots * a_{n-1} * a_n)^{-1} &= ((a_1 * \cdots * a_{n-1}) * a_n)^{-1} = a_n^{-1} * (a_1 * \cdots * a_{n-1})^{-1} \\ &= a_n^{-1} * a_{n-1}^{-1} \cdots * a_1^{-1} \end{aligned}$$

Lo que demuestra la proposición. $\blacksquare$

Ejemplos C Veamos cuales son las unidades en algunas operaciones binarias estudiadas:

$\star$ En $(\mathbb{N}, \cdot)$ sólo 1 es unidad. En $(\mathbb{Z}, \cdot)$ las unidades son $\{1, -1\}$.

$\star$ En $(\mathbb{Q}, \cdot)$ o $(\mathbb{R}, \cdot)$ las unidades son, respectivamente $\mathbb{Q} - \{0\}$ y $\mathbb{R} - \{0\}$.

$\star$ Para $(\Delta, \circ)$ con $\Delta = \{f \mid f : X \to X\}$ y $\circ$ la composición, las unidades son las aplicaciones biyectivas.

$\star$ En $(\mathbb{Z}_n, \cdot)$ las unidades son los elementos $\overline{a} \in \mathbb{Z}_n$ tales que $\mathrm{m.\,c.\,d}(n, a) = 1$.

$\star$ En $(\mathcal{M}_n(\mathbb{R}), +)$, suma de matrices, todo elemento es unidad, mientras que en $(\mathcal{M}_n(\mathbb{R}), \cdot)$ las matrices de determinante no nulo (las inversibles) son las unidades.

$\star$ Sea X un conjunto no vacio. En $(\mathcal{P}(X), \cup)$ sólo $\emptyset$, que es el elemento neutro, es unidad. En $(\mathcal{P}(X), \cap)$ sólo X, que es el elemento neutro, es unidad. En $(\mathcal{P}(X), \triangle)$, todo elemento es unidad. ¿Quien es el elemento neutro?

2. Nociones básicas sobre Anillos

2.1. Definiciones y ejemplos

Definición 1 Sea G un conjunto no vacío y $*$ una operación en G. Diremos que $(G, *)$ es un **grupo** si:

- $*$ es asociativa.
- $*$ tiene elemento unidad, normalmente denotado por e.
- Todo elemento de G tiene inverso.

Si además $*$ es conmutativa se dirá que G es un **grupo abeliano**.

Ejemplos A $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$ son grupos abelianos respecto de la suma. $\mathbb{Q} - \{0\}$ y $\mathbb{R} - \{0\}$ son grupos abelianos respecto del producto. $(\mathcal{P}(X), \triangle)$ es un grupo abeliano para cualquier conjunto no vacío X. El conjunto de las matrices inversibles en $\mathcal{M}_2(\mathbb{R})$ con el producto es un grupo no abeliano.

Fin de clase 16; 11-11-2011, grupo A y B

Definición 2 Un **anillo** es una terna $(R, +, \cdot)$ en donde R es un conjunto y "+", "$\cdot$" son dos operaciones en R tales que:

(1) $(R, +)$ es un grupo abeliano:

- Propiedad asociativa: $(a + b) + c = a + (b + c)$ para todo $a, b, c \in R$.
- Elemento neutro: existe $0 \in R$ tal que $a + 0 = 0 + a$ para todo $a \in R$
- Elemento opuesto: para todo $a \in R$ existe $-a \in R$ tal que

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

- Propiedad conmutativa: $a + b = b + a$ para todo $a, b \in R$.

(2) $(R, \cdot)$ verifica la propiedad asociativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para todo $a, b, c \in R$.

(3) Se verifican las propiedades distributivas: para todos $a, b, c \in R$,

$$(a+b)\cdot c = a\cdot c + b\cdot c \qquad c\cdot(a+b) = c\cdot a + c\cdot b$$

⋆ Diremos que un **anillo** $(R, +, \cdot)$ es **conmutativo** si "$\cdot$" es conmutativa.
⋆ Diremos que un **anillo** $(R, +, \cdot)$ es **unitario** si "$\cdot$" es una operación unitaria y R tiene más de un elemento (0 y 1 son dos elementos distintos de R).

Nota: La primera operación se llamará **suma**. El neutro de la suma lo denotaremos por 0. Al inverso de la suma lo llamaremos **Opuesto**. La segunda operación se llamará **producto** y la denotaremos por yuxtaposición. Al neutro del producto lo denotaremos, si existe, por 1. El inverso del producto, si existe, se llamará **inverso**.

Ejemplos B

- Si consideramos $(G, +)$ un grupo abeliano y definimos un producto en G por: $a \cdot b := 0$ para todo $a, b \in G$, $(G, +, \cdot)$ tiene estructura de anillo conmutativo.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con las operaciones usuales (todos son anillos conmutativos y unitarios). $\mathcal{M}_n(\mathbb{R})$, el anillo de matrices sobre los Reales, con las operaciones usuales (anillo unitario, no conmutativo para $n \geq 2$). $2\mathbb{Z}$ con las operaciones usuales de $\mathbb{Z}$ (anillo conmutativo no unitario).
- Los anillos realmente no tienen que ser de "números": sea X un conjunto no vacío y denotemos por $\mathcal{P}(X)$ el conjunto de partes de X. Entonces $(\mathcal{P}(X), \triangle, \cap)$ tiene estructura de anillo conmutativo y unitario.

  Nota: $\triangle$ denota la diferencia simétrica: dados $A, B \subset X$,

  $$A \triangle B := (A - B) \cup (B - A) = (A \cap B^c) \cup (B \cap A^c)$$

- Los anillos módulo n: Sea n un número natural y consideremos

  $$\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}.$$

  Observar que $\mathbb{Z}_n$ tiene n elementos. Dados $a, b \in \mathbb{Z}_n$ definimos:

  - La suma de a y b como el resto de dividir $a + b$ por n.
    ⋆ $(\mathbb{Z}_n, +)$ es el grupo abeliano ya estudiado anteriormente.
  - El producto de a y b como el resto de dividir $a \cdot b$ por n.
    Entonces $(\mathbb{Z}_n, +, \cdot)$ tiene estructura de anillo conmutativo y unitario, $n \geq 2$.

Proposición 3 Sea $(R, +, \cdot)$ un anillo. Entonces:

(i) $0 \cdot a = a \cdot 0 = 0$ para todo $a \in R$.

(ii) $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$ para todo $a, b \in R$.
Si además R es unitario,

(iii) la unidad es única.

(iv) Si $a \in R$ es un elemento inversible, el inverso de a es único (lo denotamos por a^{-1}).

Demo: (i). Sabemos que al ser 0 el neutro de la suma, $0+0=0$. Por tanto,

$$0a = (0+0)a = 0a + 0a$$

Simplemente hemos aplicado la distributiva de la suma. Ahora, Si sumamos en ambos lados de la igualdad el opuesto de $0a$ tenemos,

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

El caso $a0 = 0$ se demuestra de forma análoga.

(ii). Queremos ver que $a(-b) = -(ab)$, es decir, que a por el opuesto de b es el opuesto de ab. Pero

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

por lo que cuando a ab le sumo $a(-b)$ me da cero. Esto nos dice exactamente que el opuesto de a es $a(-b)$ (ya que el opuesto es único), es decir, $-(ab) = a(-b)$. de forma análoga se demuestra que $-(ab) = (-a)b$.

(iii) y (iv). Sabemos que en cualquier operación, en particular para el producto de un anillo R la unidad caso de existir es única y el inverso de un elemento, caso de existir, es único. ■

Corolario 4 (Ejercicio) Sea $(R, +, \cdot)$ un anillo unitario. Entonces $0 \neq 1$.

Ejemplos C *A los elementos inversibles de un anillo R se les denomina unidades. El conjunto de las unidades de un anillo R se denota por $\mathcal{U}(R)$.*

Corolario 5 (Ejercicio) Sea $(R, +, \cdot)$ un anillo unitario. Entonces $(\mathcal{U}(R), \cdot)$ tiene estructura de grupo. Es más, si R es conmutativo, $\mathcal{U}(R)$ es un grupo abeliano.

Definición 6 Se dice que un anillo $(R, +, \cdot)$ es un **anillo de división** si es unitario y todo elemento no nulo de R tiene inverso. Si además es conmutativo, se dice que $(R, +, \cdot)$ es un **cuerpo**.

Nota: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son cuerpos. Si p es un número primo, $\mathbb{Z}_p$, el anillo de congruencias módulo p, es un cuerpo (se ha demostrado en el corolario 7 (Pag. 42)).

Propiedades 7 Vamos a pensar ahora en una propiedad que normalmente hemos usado en los anillos "de números" ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$): si $a \cdot b = 0$, entonces $a = 0$ o $b = 0$. Curiosamente esta propiedad no es cierta en todo anillo: Veamos varios contraejemplos:

(1) Si consideramos las matrices de tamaño n (con $n \in \mathbb{N}$, $n \geq 2$) tenemos que $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$, las matrices con su suma y producto usual tienen estructura de anillo (anillo unitario, no conmutativo si $n > 1$). Y ya sabemos que podemos tener dos matrices no nulas de producto cero:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 5 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

(2) Podemos considerar algunos anillos de congruencias modulo n, que son conmutativos y unitarios, $(\mathbb{Z}_n, +, \cdot)$: Por ejemplo, en $\mathbb{Z}_{12}$,

$$\bar{6} \cdot \bar{4} = \bar{0} \text{ pero } \bar{6} \neq \bar{0} \text{ y } \bar{4} \neq \bar{0}$$

Definición 8 Sea R un anillo. Se dice que un elemento no nulo $a \in R$ es:

- Un **divisor de cero por la izquierda** si existe $0 \neq b \in R$ tal que $a \cdot b = 0$.
- Un **divisor de cero por la derecha** si existe $0 \neq b \in R$ tal que $b \cdot a = 0$.

Un anillo conmutativo y unitario sin divisores de cero por la izquierda y por la derecha se denomina un **dominio de integridad** (normalmente denotaremos los dominios de integridad por D.I.)

Corolario 9 (ejercicio) Sea $(R, +, \cdot)$ un anillo y sea a un elemento inversible de R. Entonces a no es divisor de cero (ni por la izquierda ni por la derecha) en R.

Corolario 10 (ejercicio) Todo cuerpo es un dominio de integridad. $\mathbb{Z}$ es un D.I. que no es cuerpo.

Definición 11 Se dice que un anillo R verifica la **ley de cancelación por la izquierda** si para todo elemento no nulo $a \in R$ y para todos $x, y \in R$ se verifica que

$$ax = ay \quad \Longrightarrow \quad x = y.$$

Se dice que un anillo R verifica la **ley de cancelación por la derecha** si para todo elemento no nulo $a \in R$ y para todos $x, y \in R$ se verifica que

$$xa = ya \quad \Longrightarrow \quad x = y.$$

Proposición 12 (ejercicio) Sea $(R, +, \cdot)$ un anillo. Las siguientes condiciones son equivalentes:

(i) R no posee divisores de cero por la izquierda (Resp. derecha).

(ii) Se verifican las leyes de cancelación por la izquierda (Resp. derecha).

Corolario 13 (ejercicio) Para un anillo conmutativo y unitario $(R, +, \cdot)$ las siguientes condiciones son equivalentes:

(i) R es un dominio de integridad.

(ii) Se verifican las leyes de cancelación en R. Es decir,

$$\text{Si } ax = ay \text{ con } a \neq 0, \text{ entonces } x = y$$

Nota: Sólo hemos escrito una de las leyes de cancelación ya que el anillo es conmutativo, con lo que la otra es inmediata.

★ Los ejercicios del 1 al 15 te pueden servir para saber si has asimilado los conceptos de esta sección.

2.2. Subanillos

Definición 14 *Sea $(R, +, \cdot)$ un anillo. Se dice que $A \subset R$ es un subanillo de R, y se representa $A \leq R$, si:*

- *La suma de R es una operación interna en A: $a + b \in A$ para todos $a, b \in A$.*
- *El producto de R es una operación interna en A: $a \cdot b \in A$ para todos $a, b \in A$.*
- *$(A, +, \cdot)$ tiene estructura de anillo.*

Nota: Observar que los dos primeros puntos significan que la suma y el producto de R definen operaciones en A.

Nota: Por tanto, para demostrar que un subconjunto A de un anillo R es un subanillo tenemos que demostrar 9 propiedades. No obstante algunas son triviales:

Fin de clase 17; 14-11-2011, grupo A y B. Primera clase recuperada

Teorema 15 Sea $(R, +, \cdot)$ un anillo y sea $A \subset R$. Entonces A es un subanillo de R si y sólo si:

(i) La suma de R es una operación interna en A: $a + b \in A$ para todos $a, b \in A$.
(ii) $0 \in A$.
(iii) Para todo $a \in A$, $-a \in A$.
(iv) El producto de R es una operación interna en A: $a \cdot b \in A$ para todos $a, b \in A$

Demo: Supongamos en primer lugar que A es un subconjunto de R que verifica las propiedades (i), (ii) y (iii). Entonces,

★ $(A, +)$ es un grupo abeliano:

• (i) nos dice que la suma define una operación en A.

• Como se verifica (ii), $0 \in A$ y por tanto 0 es el elemento neutro de A (si para todo elemento x de R se tiene que $x + 0 = 0 + x = x$, para todo elemento a de A, que en particular es un elemento de R, se tiene que $a + 0 = 0 + a = a$).

• Si $a \in A$, por (ii), $-a \in A$ por tanto a tiene opuesto en A, el elemento $-a$.

• por ultimo, como $x + y = y + x$ para todo elemento $x, y \in R$ se tiene que esta misma propiedad se verifica para los elementos de A.

★ $(A, \cdot)$ verifica la propiedad asociativa:

• (iii) nos dice que el producto define una operación en A.

• Como $(xy)z = x(yz)$ para todo elemento $x, y, z \in R$ se tiene que esta misma propiedad se verifica para los elementos de A.

★ $(A, \cdot)$ verifica la propiedad distributiva:

• Como $(x + y)z = xz + yz$ y $z(x + y) = zx + zy$ para todo elemento $x, y, z \in R$ se tiene que estas mismas propiedades se verifican para los elementos de A.

Por tanto, si se verifica (i), (ii) y (iii) $(A, +, \cdot)$ tiene estructura de anillo, lo que implica que es subanillo de R. Veamos el recíproco.

Supongamos ahora que la suma y el producto de R dotan a A de estructura de anillo. En primer lugar, la suma es una operación en A, por lo que para todo $a, b \in A$ $a + b \in A$. De forma similar, el producto es una operación en A por lo que para todo $a, b \in A$ $a \cdot b \in A$. Es decir, se satisfacen (i) y (iii) del enunciado.

Veamos que también se satisface (ii). En primer lugar demostremos que $0 \in A$: Por hipótesis $(A, +)$ tiene estructura de grupo abeliano, por lo que posee un elemento neutro.

Denotémoslo por $0' \in A$ (en principio nadie nos dice que tenga que ser el elemento neutro de la suma de R, que denotamos por 0). Ahora, $0' = 0' + 0'$ ya que $0'$ es el neutro de $(A, +)$ pero $0' + 0 = 0'$ ya que 0 es el neutro de R. Por tanto,

$$0' + 0 = 0' + 0'.$$

Si sumamos en esta expresión por el opuesto de $0'$ en R tenemos $0 = -0' + 0' + 0 = -0' + 0' + 0' = 0' \in A$.

Demostremos ahora que para cada $a \in A$, $-a \in A$: dado $a \in A$, como $(A, +)$ es un grupo abeliano, a tiene su opuesto en A, denotémoslo por a', así,

$$a + a' = a' + a = 0 \qquad \clubsuit$$

(ya que hemos visto que el neutro de $(A, +)$ era el 0). Pero $\clubsuit$ nos dice que a' es el opuesto de a en R, es decir, que $a' = -a$. ■

Ejemplos D $2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Lema 16 (ejercicio) Un subanillo de un anillo unitario no tiene que ser unitario. Es más, aunque sea unitario la unidad del anillo y del subanillo no tiene que coincidir.

Nota: Aunque la unidad de R, si existe, (el elemento neutro del producto de R) no tiene que pertenecer al subanillo, el neutro de la suma si pertenece a cualquier subanillo, por lo que R y cualquier subanillo suyo tienen el mismo neutro para la suma.

Lema 17 (ejercicio) Todo subanillo unitario de un dominio de integridad es un dominio de integridad. En particular, todo subanillo unitario de un cuerpo es un dominio de integridad.

★ Los ejercicios del 16 al 19 te pueden servir para saber si has asimilado los conceptos de esta sección.

3. Homomorfismos de anillos

Definición 1 Sean $(R, +, .)$ y $(R', +', .')$ dos anillos. Se define un **homomorfismo** de R en R' como una aplicación $f : R \to R'$ tal que:

$$f(a + b) = f(a) +' f(b) \quad \text{para todo } a, b \in R,$$
$$f(a \cdot b) = f(a) \cdot' f(b) \quad \text{para todo } a, b \in R.$$

- Si f es inyectiva, se dice que f es un **monomorfismo**.
- Si f es sobreyectiva, se dice que f es un **epimorfismo**.
- Si f es biyectiva, se dice que f es un **isomorfismo**. En este caso se dice que los anillos R y R' son **isomorfos**.
- Si $R = R'$, se dice que f es un **endomorfismo**.
- Un endomorfismo biyectivo se le denomina un **automorfismo**.
- Si R y R' son dos anillos unitarios, diremos que $f : R \to R'$ es un **homomorfismos de anillos unitarios** si $f(1_R) = 1_{R'}$.

Proposición 2 Sean R y R' dos anillos y sea a un elemento invertible de R (con inverso a^{-1}). Entonces:

- La aplicación nula, $f : R \to R'$ definida por $f(x) = 0'$ para todo $x \in R$ es un homomorfismo de anillos.
- La aplicación identidad, $\mathrm{Id} : R \to R$ definida por $\mathrm{Id}(x) = x$ para todo $x \in R$ es un automorfismo de anillos.
- La aplicación $f_a : R \to R$ definido por $f_a(x) = a^{-1}xa$ es un automorfismo de R. Llamado el **automorfismo interno** asociado al elemento inversible a.

Demo: (1). Veamos que la aplicación $f : R \to R'$ definida por $f(x) = 0'$ para todo $x \in R$ es un homomorfismo de anillos:

$$f(x+y) = 0 = 0+0 = f(x)+f(y) \quad \text{y} \quad f(xy) = 0 = 0 \cdot 0 = f(x) \cdot f(y)$$

(2). Veamos que la aplicación identidad es un homomorfismo de anillos:

$$\mathrm{Id}(x+y) = x+y = \mathrm{Id}(x)+\mathrm{Id}(y) \quad \text{y} \quad \mathrm{Id}(x \cdot y) = x \cdot y = \mathrm{Id}(x) \cdot \mathrm{Id}(y)$$

(3). Por último demostremos que f_a verifica las propiedades que tienen que verificar los automorfismos de anillos:

$$f_a(x+y) = a^{-1}(x+y)a = a^{-1}xa + a^{-1}ya = f_a(x) + f_a(y)$$
$$f_a(x \cdot y) = a^{-1}xya = a^{-1}x(aa^{-1})ya = a^{-1}xaa^{-1}ya = f_a(x) \cdot f_a(y)$$

Es más la aplicación inversa de f_a es $f_{a^{-1}}$ en donde $f_{a^{-1}}(x) = (a^{-1})^{-1}xa^{-1} = axa^{-1}$ ya que

$$f_a \circ f_{a^{-1}}(x) = f_a(axa^{-1}) = a^{-1}(axa^{-1})a = x$$
$$f_{a^{-1}} \circ f_a(x) = f_{a^{-1}}(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x$$

Lo que demuestra el ejemplo. ■

Lema 3 Sean R y R' son dos anillos y $f : R \to R'$ un homomorfismo de anillos. Entonces:

(i) $f(0) = 0$.
(ii) $f(-a) = -f(a)$

Demo: (i). Ya hemos hecho alguna demostración con la misma idea.

$$f(0) = f(0+0) = f(0) + f(0)$$

Si ahora sumamos en ambos lados el opuesto de $f(0)$ en R' tenemos,

$$0' = f(0) - f(0) = f(0) + f(0) - f(0) = f(0)$$

(ii). Sea $a \in R$. Entonces

$$f(a) + f(-a) = f(a+(-a)) = f(0) = 0 \quad \text{y} \quad f(-a) + f(a) = f((-a)+a) = f(0) = 0$$

Por tanto el opuesto de $f(a)$ en R' es $f(-a)$. ■

Lema 4 (Ejercicio) No tiene que suceder que si R y R' son anillos unitarios, $f(1) = 1'$.

Proposición 5 Sean R y R' dos anillos, S un subanillo de R, S' un subanillo de R' y $f : R \to R'$ un homomorfismo de anillos. Entonces

(i) $f(S)$ es un subanillo de R'.
(ii) $f^{-1}(S') := \{r \in R |\ f(r) \in S'\}$ es un subanillo de R.

Demo: (i). ★ Tenemos que ver que la suma es una operación interna en $f(S)$:
Sean $x, y \in f(S)$. Entonces existen $a, b \in S$ tales que $x = f(a)$ e $y = f(b)$. Por tanto

$$x + y = f(a) + f(b) = f(a + b) \in f(S),$$

ya que como S es un subanillo de R, $a + b \in S$.

★ Tenemos que ver que el producto es una operación interna en $f(S)$:
Sean $x, y \in f(S)$. Entonces existen $a, b \in S$ tales que $x = f(a)$ e $y = f(b)$. Por tanto

$$x \cdot y = f(a) \cdot f(b) = f(a \cdot b) \in f(S),$$

ya que como S es un subanillo de R, $a \cdot b \in S$.

★ Por último, como $0 \in S$ (ya que S es un subanillo de R) $0' = f(0) \in f(S)$ y dado $x \in f(S)$ existe $a \in S$ tal que $x = f(a)$, por tanto $-x = -f(a) = f(-a) \in f(S)$, ya que $-a \in S$.

(ii). ★ Tenemos que ver que la suma es una operación interna en $f^{-1}(S')$:
Sean $a, b \in f^{-1}(S')$ (por definición $f(a), f(b) \in S'$). Entonces $f(a + b) = f(a) + f(b) \in S'$ ya que S' es un subanillo de R'.

★ Tenemos que ver que el producto es una operación interna en $f^{-1}(S')$:
Sean $a, b \in f^{-1}(S')$ (por definición $f(a), f(b) \in S'$). Entonces $f(a \cdot b) = f(a) \cdot f(b) \in S'$ ya que S' es un subanillo de R'.

★ Por último, $f(0) = 0' \in S'$ (ya que S' es subanillo de R') y por tanto $0 \in f^{-1}(S')$. Por último, si $a \in f^{-1}(S')$ (es decir, $f(a) \in S'$), $f(-a) = -f(a) \in S'$ y por tanto $-a \in f^{-1}(S')$. ■

Corolario 6 Sean R y R' dos anillos, S un subanillo de R, S' un subanillo de R' y $f : R \to R'$ un homomorfismo de anillos. Entonces:

(i) $\mathrm{Ker}(f) := f^{-1}(0)$, llamado el **núcleo o Ker** de f, es un subanillo de R.

(ii) $\mathrm{Im}(f) := f(R)$, llamada la **imagen** de f, es un subanillo de R'.

Nota: Cuando lleguemos a la estructura cociente en anillo veremos que $\mathrm{Ker}(f)$ tiene propiedades mucho más interesantes que la de ser simplemente un subanillo.

Fin de clase 18; 15-11-2011, grupo A y B.

Proposición 7 Sean R y R' dos anillos, S un subanillo de R, S' un subanillo de R' y $f : R \to R'$ un homomorfismo de anillos. Entonces

(i) f es un monomorfismo si y sólo si $\mathrm{Ker}(f) = 0$.
(ii) f es un epimorfismo si y sólo si $\mathrm{Im}(f) = R'$.

Demo: (i). Recordamos que $\mathrm{Ker}(f) = \{a \in R \mid f(a) = 0'\}$. Por tanto, si f es inyectiva sólo el cero puede ir al cero y por tanto $\mathrm{Ker}(f) = \{0\}$. Recíprocamente, supongamos que $\mathrm{Ker}(f) = \{0\}$ y sean $a, b \in R$ tales que $f(a) = f(b)$. Entonces

$$0' = f(a) + (-f(b)) = f(a - b)$$

por lo que $a - b \in \mathrm{Ker}(f) = \{0\}$ y por tanto $a - b = 0$, es decir, $a = b$.

(ii). es una consecuencia de ser f aplicación (no intervienen las nociones de anillo para demostrar esto). ■

Proposición 8 *Sean $(R, +, .)$ y $(R', +', .')$ dos anillos y $f : R \to R'$ un isomorfismo de anillos. Entonces $f^{-1} : R' \to R$ también es un isomorfismo de anillos.*

Cada estructura que demos en algebra tendrá su homomorfismo asociado. Por ejemplo, la noción de subanillo está ligada con la noción de monomorfismo:

Proposición 9 Sea R un subanillo de R'. Entonces la inclusión de R en R', $i : R \hookrightarrow R'$ definida por $i(r) = r$ es un monomorfismo de anillos. Es más: si $f : R \to R'$ es un monomorfismo de anillos, entonces R es isomorfo a $\mathrm{Im}(f) \leq R'$ (por lo que se puede considerar que R es un subanillo de R').

En la proxima sección vemos más homomorfismos asociados a distintas construcciones de anillos.

★ Los ejercicios del 20 al 28 te pueden servir para saber si has asimilado los conceptos de esta sección.

4. Construcción de nuevos anillos

4.1. El producto directo de anillos.

Proposición 1 Sea I un conjunto de indices y R_i, $i \in I$ una familia de anillos. Entonces $\Pi_{i \in I} R_i$ Tiene estructura de anillo con la suma y el producto definidos por componentes:

$$\Pi_{i \in I} R_i := \{(r_i)_{i \in I} \quad \text{con} \quad r_i \in R_i, \quad i \in I\}$$

⋆ Con suma: $(r_i)_{i \in I} + (r'_i)_{i \in I} = (r_i + r'_i)_{i \in I}$
⋆ y producto, $(r_i)_{i \in I} \cdot (r'_i)_{i \in I} = (r_i \cdot r'_i)_{i \in I}$

Ejemplos A *Veamos un ejemplo antes de demostrar la proposición. Sean los anillos $\mathbb{Z}_2$ y $\mathbb{Z}_3$. Entonces la proposición anterior nos dice que*

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\overline{a}, \overline{b}) \mid \overline{a} \in \mathbb{Z}_2 \ y \ \overline{b} \in \mathbb{Z}_3\} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2})\}$$

Con suma y producto por componentes, por ejemplo,

$$(\overline{0}, \overline{2}) + (\overline{1}, \overline{0}) = (\overline{0} + \overline{1}, \overline{2} + \overline{0}) = (\overline{1}, \overline{2})$$
$$(\overline{0}, \overline{2}) \cdot (\overline{1}, \overline{0}) = (\overline{0} \cdot \overline{1}, \overline{2} \cdot \overline{0}) = (\overline{0}, \overline{0})$$

Demo: (Proposición 1 (Pag. 63)) Es claro que la suma y el producto en $\Pi_{i\in I}R_i$ están bien definidos ya que si $(r_i)_{i\in I}, (r'_i)_{i\in I} \in \Pi_{i\in I}R_i$, para cada $i \in I$, r_i e $r'_i \in R_i$ y por tanto $r_i + r'_i \in R_i$ y $r_i \cdot r'_i \in R_i$, por lo que $(r_i + r'_i)_{i\in I}, (r_i \cdot r'_i)_{i\in I} \in \Pi_{i\in I}R_i$. Veamos ahora que se verifica que $(\Pi_{i\in I}R_i, +, \cdot)$ tiene estructura de anillo:

★ $(\Pi_{i\in I}R_i, +)$ tiene estructura de grupo abeliano:

⋆ Asociativa: sean $(x_i)_{i\in I}, (y_i)_{i\in I}$ y $(z_i)_{i\in I} \in \Pi_{i\in I}R_i$. Entonces,

$$\begin{aligned}[(x_i)_{i\in I} + (y_i)_{i\in I}] + (z_i)_{i\in I} &= (x_i + y_i)_{i\in I} + (z_i)_{i\in I} = ([x_i + y_i] + z_i)_{i\in I} \\ &= (x_i + [y_i + z_i])_{i\in I} = (x_i)_{i\in I} + (y_i + z_i)_{i\in I} \\ &= (x_i)_{i\in I} + [(y_i)_{i\in I} + (z_i)_{i\in I}].\end{aligned}$$

⋆ Conmutativa: sean $(x_i)_{i\in I}$ e $(y_i)_{i\in I} \in \Pi_{i\in I}R_i$. Entonces,

$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I} = (y_i + x_i)_{i\in I} = (y_i)_{i\in I} + (x_i)_{i\in I}$$

⋆ Neutro: sea $(x_i)_{i\in I} \in \Pi_{i\in I}R_i$ y consideremos $0_i \in R_i$ el neutro del anillo R_i. Entonces,

$$\begin{aligned}(x_i)_{i\in I} + (0_i)_{i\in I} &= (x_i + 0_i)_{i\in I} = (x_i)_{i\in I} \\ (0_i)_{i\in I} + (x_i)_{i\in I} &= (0_i + x_i)_{i\in I} = (x_i)_{i\in I}\end{aligned}$$

Por tanto el neutro para la suma en $\Pi_{i\in I}R_i$ es $(0_i)_{i\in I}$.

⋆ Opuesto: sea $(x_i)_{i\in I} \in \Pi_{i\in I}R_i$. Para cada $k \in I$ sea x_k (el elemento de R_k que está en la coordenada k). Sea $-x_k$ su opuesto en R_k y consideremos $(-x_i)_{i\in I} \in \Pi_{i\in I}R_i$. Entonces,

$$\begin{aligned}(x_i)_{i\in I} + (-x_i)_{i\in I} &= (x_i - x_i)_{i\in I} = (0_i)_{i\in I} \\ (-x_i)_{i\in I} + (x_i)_{i\in I} &= (-x_i + x_i)_{i\in I} = (0_i)_{i\in I}\end{aligned}$$

Por tanto el opuesto de $(x_i)_{i\in I}$ en $\Pi_{i\in I}R_i$ es $(-x_i)_{i\in I} \in \Pi_{i\in I}R_i$.

★ $(\Pi_{i\in I}R_i, \cdot)$ es asociativa: sean $(x_i)_{i\in I}, (y_i)_{i\in I}$ y $(z_i)_{i\in I} \in \Pi_{i\in I}R_i$. Entonces,

$$\begin{aligned}[(x_i)_{i\in I} \cdot (y_i)_{i\in I}] \cdot (z_i)_{i\in I} &= (x_i \cdot y_i)_{i\in I} \cdot (z_i)_{i\in I} = ([x_i \cdot y_i] \cdot z_i)_{i\in I} \\ &= (x_i \cdot [y_i \cdot z_i])_{i\in I} = (x_i)_{i\in I} \cdot (y_i \cdot z_i)_{i\in I} \\ &= (x_i)_{i\in I} \cdot [(y_i)_{i\in I} \cdot (z_i)_{i\in I}].\end{aligned}$$

★ $(\Pi_{i\in I}R_i, +, \cdot)$ verifica la distributiva: sean $(x_i)_{i\in I}, (y_i)_{i\in I}$ y $(z_i)_{i\in I} \in \Pi_{i\in I}R_i$. Entonces,

$$\begin{aligned}[(x_i)_{i\in I} + (y_i)_{i\in I}] \cdot (z_i)_{i\in I} &= (x_i + y_i)_{i\in I} \cdot (z_i)_{i\in I} = ([x_i + y_i] \cdot z_i)_{i\in I} \\ &= (x_i \cdot z_i + y_i \cdot z_i)_{i\in I} = (x_i \cdot z_i)_{i\in I} + (y_i \cdot z_i)_{i\in I} \\ &= (x_i)_{i\in I} \cdot (z_i)_{i\in I} + (y_i)_{i\in I} \cdot (z_i)_{i\in I}. \\ (z_i)_{i\in I} \cdot [(x_i)_{i\in I} + (y_i)_{i\in I}] &= (z_i)_{i\in I} \cdot (x_i + y_i)_{i\in I} = (z_i \cdot [x_i + y_i])_{i\in I} \\ &= (z_i \cdot x_i + z_i \cdot y_i)_{i\in I} = (z_i \cdot x_i)_{i\in I} + (z_i \cdot y_i)_{i\in I} \\ &= (z_i)_{i\in I} \cdot (x_i)_{i\in I} + (z_i)_{i\in I} \cdot (y_i)_{i\in I}.\end{aligned}$$

Por tanto $(\Pi_{i\in I}R_i, +, \cdot)$ tiene estructura de anillo. ■

El producto directo de anillos está ligado a la noción de proyección canónica y a cierta propiedad estructural:

Definición 2 Sean $R_i,\ i \in I$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los R_i. Se define la **proyección "canónica"** de R en R_k, con $k \in I$, como:

$$\begin{array}{rccc} \pi_k : & R & \longrightarrow & R_k \\ & (r_i)_{i\in I} & \longmapsto & r_k. \end{array}$$

Proposición 3 (ejercicio) Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los R_i. Entonces, para cada $k \in I$, la proyección canónica $\pi_k : \Pi_{i\in I} R_i \to R_k$ es un epimorfismo de anillos.

Proposición 4 (ejercicio) Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los R_i. Entonces,

- R es unitario si y sólo si R_k es unitario para todo $k \in I$.
- R es conmutativo si y sólo si R_k es conmutativo para todo $k \in I$.
- Si $\#I \geq 2$ y ningún anillo es el anillo nulo, $(\{0\}, +, \cdot)$, R tiene divisores de cero. Por tanto, en este caso, R no puede ser dominio de integridad, ni anillo de división ni cuerpo.

Fin de clase 19; 16-11-2011, grupo A. Segunda clase recuperada

4.2. La suma directa de anillos.

Proposición 5 Sea I un conjunto de indices y $\{R_i\}_{i\in I}$ una familia de anillos. Entonces

$$\bigoplus_{i\in I} R_i = \{(r_i)_{i\in I} \in \Pi_{i\in I} R_i \mid r_i = 0 \quad \text{para casi todo } i\}$$

es un subanillo de $\Pi_{i\in I} R_i$, llamado la **suma directa externa** de los R_i
Nota: Al ser un subanillo la suma y el producto se definen por componentes:
⋆ Suma por componentes: $(r_i)_{i\in I} + (r'_i)_{i\in I} = (r_i + r'_i)_{i\in I}$
⋆ Producto por componentes: $(r_i)_{i\in I} \cdot (r'_i)_{i\in I} = (r_i \cdot r'_i)_{i\in I}$

Demo: Es claro que si sumo o multiplico dos elementos del producto con un número finito de coordenadas no nulas, obtengo un elemento con un número finito de coordenadas no nulas, ver la proposición 1 (Pag. 63) para la definición de producto directo de anillos. Es más,
⋆ $(0_i) \in \bigoplus_{i\in I} R_i$ (el elemento neutro de la suma de $\Pi_{i\in I} R_i$) y
⋆ si $(r_i)_{i\in I} \in \bigoplus_{i\in I} R_i$, su opuesto (respecto de la suma en $\Pi_{i\in I} R_i$) es $(-r_i)_{i\in I}$ que pertenece a $\bigoplus_{i\in I} R_i$.
Por tanto, por el teorema 15 (Pag. 59), $\bigoplus_{i\in I} R_i \leq \Pi_{i\in I} R_i$. ■

Nota: Si $\#I < \infty$ se tiene que la suma directa y el producto directo coinciden.

Definición 6 Sean $\{R_i\}_{i\in I}$ una familia de anillos y sea $\bigoplus_{i\in I} R_i$ la suma directa de éstos. Entonces para cada $k \in I$ se define la **inclusión canónica** de R_k en $\bigoplus_{i\in I} R_i$ y se representa por

$$\rho_k : R_k \to \bigoplus_{i\in I} R_i$$

como $\rho_k(r_k) = (x_i)_{i\in I}$ en donde $x_i = 0$ si $i \neq k$ y $x_k = r_k$. Es decir, la upla de $\Pi_{i\in I} R_i$ que tiene todas las coordenadas cero, salvo la k que vale r_k.

Proposición 7 (ejercicio) Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \bigoplus_{i\in I} R_i$ la suma directa de los R_i. Entonces, para cada $k \in I$, la inclusión canónica $\rho_k : R_k \to \bigoplus_{i\in I} R_i$ es un monomorfismo de anillos.

4.3. El anillo de matrices

Proposición 8 Sea R un anillo y $n \in \mathbb{N}$. Entonces El conjunto $\mathcal{M}_n(R)$ definido como:

$$\mathcal{M}_n(R) := \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \quad \text{con } a_{ij} \in R \text{ para } i,j = 1,2,\ldots,n \right\}$$

con su suma definida por componentes y producto habitual de matrices tiene estructura de anillo. Es decir, dadas

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \qquad B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

Nota: En notación reducida, $A = (a_{ij})$ y $B = (b_{ij})$.

- $A + B = (a_{ij} + b_{ij}) = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \cdots & a_{nn}+b_{nn} \end{pmatrix}$

- $A \cdot B = (\sum_{k=1}^n a_{ik} \cdot b_{kj}) = \begin{pmatrix} \sum_{k=1}^n a_{1k}\cdot b_{k1} & \sum_{k=1}^n a_{1k}\cdot b_{k2} & \cdots & \sum_{k=1}^n a_{1k}\cdot b_{kn} \\ \sum_{k=1}^n a_{2k}\cdot b_{k1} & \sum_{k=1}^n a_{2k}\cdot b_{k2} & \cdots & \sum_{k=1}^n a_{2k}\cdot b_{kn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^n a_{nk}\cdot b_{k1} & \sum_{k=1}^n a_{nk}\cdot b_{k2} & \cdots & \sum_{k=1}^n a_{nk}\cdot b_{kn} \end{pmatrix}$

Demo: ★ Es claro que la suma es una operación bien definida en $\mathcal{M}_n(R)$. Es más, la suma se define componente a componente, por lo que (siguiendo la demostración del producto cartesiano de anillos), $(\mathcal{M}_n(R), +)$ es un grupo abeliano. Observar que el elemento neutro para la suma es

$$0 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

y el opuesto para un elemento $A = (a_{ij}) \in \mathcal{M}_n(R)$ es $-A = (-a_{ij})$.

★ Es claro que el producto es una operación bien definida en $\mathcal{M}_n(R)$. Algo más complicado será demostrar la propiedad asociativa. Usemos la notación reducida:

$$(A \cdot B) \cdot C = (\sum_{r=1}^{n} a_{ir} \cdot b_{rj}) \cdot (c_{ij}) = (\sum_{r,s=1}^{n} (a_{ir} \cdot b_{rs}) \cdot c_{sj})$$

$$A \cdot (B \cdot C) = (a_{ij}) \cdot (\sum_{s=1}^{n} b_{is} \cdot c_{sj}) = (\sum_{r,s=1}^{n} a_{ir} \cdot (b_{rs} \cdot c_{sj}))$$

Nota: Una demostración con notación matricial la puedes encontrar al final del tema.

★ Demostremos las propiedades distributivas. Usemos la notación reducida:

$$\begin{aligned}(A+B) \cdot C &= (a_{ij} + b_{ij}) \cdot (c_{ij}) = (\sum_{r=1}^{n} (a_{ir} + b_{ir}) \cdot c_{rj}) = (\sum_{r=1}^{n} a_{ir} \cdot c_{rj}) + (\sum_{r=1}^{n} b_{ir} \cdot c_{rj}) \\ &= A \cdot C + B \cdot C \\ A \cdot (B+C) &= (a_{ij}) \cdot (b_{ij} + c_{ij}) = (\sum_{r=1}^{n} a_{ir} \cdot (b_{rj} + c_{rj})) = (\sum_{r=1}^{n} a_{ir} \cdot b_{rj}) + (\sum_{r=1}^{n} a_{ir} \cdot c_{rj}) \\ &= A \cdot B + A \cdot C\end{aligned}$$

Proposición 9 (ejercicio) Sea R un anillo y $n \in \mathbb{N}$. Entonces

(i) $\mathcal{M}_n(R)$ es unitario si y sólo si R es unitario.
(i) $\mathcal{M}_n(R)$ tiene divisores de cero si $n \geq 2$. Por tanto, en este caso, $\mathcal{M}_n(R)$ no puede ser ni dominio de integridad, ni anillo de división ni cuerpo.
(ii) $\mathcal{M}_n(R)$ es conmutativo si y sólo si R es conmutativo y $n = 1$.
(iii) $\mathcal{M}_n(R)$ es un anillo de división si y sólo si R es un anillo de división y $n = 1$.
(iv) $\mathcal{M}_n(R)$ es un cuerpo si y sólo si R es un cuerpo y $n = 1$.

★ Los ejercicios del 29 al 33 te pueden servir para saber si has asimilado los conceptos de esta sección.

Fin de clase 20; 17-11-2011, grupo A. (Grupo B no da clases por fiesta de San Alberto). Viernes 18 no hay clases

Fin de clase 19; Lunes 21-11-2011, grupo B (recuperan el jueves)

4.4. El anillo de polinomios y el anillo de series formales

El anillo de series formales

Proposición 10 Sea R un anillo. Se define el anillo de series formales sobre R y se representa por $R[[X]]$ como el conjunto:

$$R[[X]] := \{\sum_{n=0}^{\infty} a_n X^n | \quad \text{con } a_n \in R\}$$

con suma y producto dado por:

(i) Suma por componentes: $\sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty}(a_n + b_n)X^n$.

(ii) Producto: $\sum_{n=0}^{\infty} a_n X^n \cdot \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k \cdot b_{n-k}\right) X^n$.

Demo: La suma en $R[[X]]$ coincide con la suma por componentes, por lo que la demostración de que $(R[[X]], +)$ es un grupo abeliano es la misma a la dada para demostrar que la suma en el producto cartesiano de anillos dota a éste de estructura un grupo abeliano.

★ Veamos que el producto es asociativo. Primero dos identidades:

$$(\star_1)\ \sum_{k=0}^{n}\sum_{s=0}^{n-k} a_{ks} = \sum_{k=0}^{n}\sum_{s=0}^{n-k} a_{sk}. \qquad (\star_2)\ \sum_{r=0}^{n} a_r = \sum_{r=0}^{n} a_{n-r}.$$

En $(\star_1)$ simplemente estamos reordenando los sumandos. En ambos sumatorios se suman los elementos

$$\begin{array}{ccccc} a_{00} & a_{01} & \cdots & a_{0\,n-1} & a_{0n} \\ a_{10} & a_{11} & \cdots & a_{1\,n-1} & \\ \vdots & \vdots & \iddots & & \\ a_{n-1\,0} & a_{n-1\,1} & & & \\ a_{n0} & & & & \end{array}$$

En el primer termino de $(\star_1)$ los estamos sumando por filas mientras que en el segundo término de $(\star_1)$ los estamos sumando por columnas. En $(\star_2)$ sumamos los elementos $a_1 + a_2 + \cdots + a_n$ en el primer término de la identidad y sumamos $a_n + \cdots + a_2 + a_1$ en el segundo.

$$\begin{aligned} &\star\left(\sum_{n=0}^{\infty} a_n X^n \cdot \sum_{n=0}^{\infty} b_n X^n\right) \cdot \sum_{n=0}^{\infty} c_n X^n = \sum_{n=0}^{\infty}\left(\sum_{s=0}^{n} a_s \cdot b_{n-s}\right) X^n \cdot \sum_{n=0}^{\infty} c_n X^n \\ &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\left(\sum_{s=0}^{k} a_s \cdot b_{k-s}\right) \cdot c_{n-k}\right) X^n = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\sum_{s=0}^{k} a_s \cdot b_{k-s} \cdot c_{n-k}\right) X^n \end{aligned}$$

$$\begin{aligned} &\star \sum_{n=0}^{\infty} a_n X^n \cdot \left(\sum_{n=0}^{\infty} b_n X^n \cdot \sum_{n=0}^{\infty} c_n X^n\right) = \sum_{n=0}^{\infty} a_n X^n \cdot \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} b_k \cdot c_{n-k}\right) X^n \\ &= \sum_{n=0}^{\infty}\sum_{k=0}^{n}\left(a_k \cdot \left(\sum_{s=0}^{n-k} b_s \cdot c_{n-s-k}\right)\right) X^n = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\sum_{s=0}^{n-k} a_k \cdot b_s \cdot c_{n-s-k}\right) X^n \\ &=^{(\star_2^s)} \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\sum_{s=0}^{n-k} a_k \cdot b_{n-k-s} \cdot c_s\right) X^n =^{(\star_1)} \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\sum_{s=0}^{n-k} a_s \cdot b_{n-k-s} \cdot c_k\right) X^n \\ &=^{(\star_2^*)} \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\sum_{s=0}^{k} a_s \cdot b_{k-s} \cdot c_{n-k}\right) X^n \end{aligned}$$

En donde, en $(\star_2^s)$ sumamos s desde $n-k$ a 0 (s hace el papel de r en $(\star_2)$) y en $(\star_2^k)$ sumamos k desde n a 0 (k hace el papel de r en $(\star_2)$).

★ Veamos que el producto es distributivo.

$$\star\left(\sum_{n=0}^{\infty}a_nX^n+\sum_{n=0}^{\infty}b_nX^n\right)\cdot\sum_{n=0}^{\infty}c_nX^n=\sum_{n=0}^{\infty}(a_n+b_n)X^n\cdot\sum_{n=0}^{\infty}c_nX^n=$$
$$=\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}(a_k+b_k)\cdot c_{n-k}\right)X^n=\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}a_k\cdot c_{n-k}+b_k\cdot c_{n-k}\right)X^n$$
$$=\sum_{n=0}^{\infty}a_nX^n\cdot\sum_{n=0}^{\infty}c_nX^n+\sum_{n=0}^{\infty}b_nX^n\cdot\sum_{n=0}^{\infty}c_nX^n$$

$$\star\sum_{n=0}^{\infty}c_nX^n\cdot\left(\sum_{n=0}^{\infty}a_nX^n+\sum_{n=0}^{\infty}b_nX^n\right)=\sum_{n=0}^{\infty}c_nX^n\cdot\sum_{n=0}^{\infty}(a_n+b_n)X^n=$$
$$=\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}c_k\cdot(a_{n-k}+b_{n-k})\right)X^n=\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}c_k\cdot a_{n-k}+c_k\cdot b_{n-k}\right)X^n$$
$$=\sum_{n=0}^{\infty}c_nX^n\cdot\sum_{n=0}^{\infty}a_nX^n+\sum_{n=0}^{\infty}c_nX^n\cdot\sum_{n=0}^{\infty}b_nX^n$$

Por lo que $R[[X]]$ tiene estructura de anillo. ■

Teorema 11 Sea R un anillo. Entonces la aplicación $i:R\to R[[X]]$ definida por $i(a)=a+\sum_{n=1}^{\infty}0X^n$ es un monomorfismo de anillos. Por tanto podemos considerar R como subanillo del anillo de series formales, $R\approx i(R)\leq R[[X]]$.

Proposición 12 (ejercicio) Sea R un anillo y sea $R[[X]]$ el anillo de series formales con coeficientes en R. Entonces:

(i) R es unitario si y sólo si $R[[X]]$ es unitario.

(ii) R es conmutativo si y sólo si $R[[X]]$ es conmutativo.

(ii) R es D.I si y sólo si $R[[X]]$ es D.I.

En el anillo de series formales suceden algunos hechos curiosos. Por ejemplo, si R es un anillo unitario $1+X$ es un elemento inversible de $R[[X]]$ con inverso $\sum_{n=0}^{\infty}(-1)^nX^n$. Es más:

Proposición 13 (ejercicio) Sea R un anillo unitario y sea $R[[X]]$ el anillo de series formales con coeficientes en R. Entonces un elemento $\sum_{n=0}^{\infty}a_nX^n\in R[[X]]$ es inversible si y sólo si a_0 es un elemento inversible de R.

Corolario 14 Sea $\mathbb{F}$ es un cuerpo. Entonces

$$\textstyle\sum_{n=0}^{\infty}a_nX^n\in\mathbb{F}[[X]] \text{ es inversible si y sólo si } a_0\neq 0.$$

El anillo de polinomios

Proposición 15 Sea R un anillo. Se define el anillo de polinomios con coeficientes en R, y se denota por $R[X]$ como el subanillo de $R[[X]]$ consistente en las series con sólo un número finito de coeficientes no nulos, es decir:

$$R[X] := \{\sum_{k=0}^{n} a_k X^k | \quad \text{con } n \in \mathbb{N} \text{ y } a_k \in R,\ k = 1, 2, \ldots, n\}$$

Demo: Claramente la suma y el producto son operaciones internas en $R[X]$. Por otro lado $0 \in R[X]$ y el opuesto de un polinomio $p(X)$ es $-p(X)$ que también pertenece a $R[X]$. ■

Definición 16 Sea R un anillo y sea $R[X]$ el anillo de polinomios con coeficientes en R. Se define el grado de un polinomio $p(X) = \sum_{k=0}^{n} a_k X^k$ y se denota por $\deg(p(X))$, como el mayor $k \in \mathbb{N}$ tal que $a_k \neq 0$.

Como corolario del Teorema 11 (Pag. 69) tenemos:

Corolario 17 R puede verse como subanillo de $R[X]$ consistente en todos los polinomios de grado cero.

Proposición 18 (ejercicio) Sea R un anillo y sea $R[X]$ el anillo de polinomios con coeficientes en R y sean $p(X), q(X) \in R[X]$. Entonces

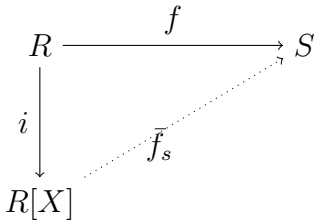
(i) R es conmutativo si y sólo si $R[X]$ es conmutativo.
(ii) R es unitario si y sólo si $R[X]$ es unitario.
(iii) R es dominio de integridad si y sólo si $R[X]$ es dominio de integridad.
(iv) $\deg(p(X) + q(X)) \leq \text{Max}(\deg(p(X)), \deg(q(X)))$.
(v) $\deg(p(X) \cdot q(X)) \leq \deg(p(X)) + \deg(q(X))$.
(vi) Es más, R no posee divisores de cero si para todo $p(X), q(X) \in R[X]$ se tiene que

$$\deg(p(X) \cdot q(X)) = \deg(p(X)) + \deg(q(X)).$$

Nota: Observar que podemos considerar R como un subanillo de $R[X]$: dado $a \in R$, podemos suponer que a es un polinomio de grado cero en $R[X]$. Más formalmente, la aplicación $i : R \to R[X]$ definida por $i(a) = a$ es un monomorfismo de anillos.

Cuando R es conmutativo nos encontramos con algunas propiedades extra en el anillo de polinomios:

Proposición 19 Sean R y S dos anillos conmutativos y sea $a \in S$. Entonces para todo homomorfismos de anillos $f : R \longrightarrow S$ existe un único homomorfismo $\bar{f}_s : R[X] \longrightarrow S$ tal que $\bar{f}_s(X) = s$ y hace conmutativo al siguiente diagrama:



Demo: Estas demostraciones tienen su estrategia de demostración. Supongamos por un momento que existe este homomorfismo de anillos $\bar{f}_s$ que hace conmutativo el diagrama (y veamos quien tiene que ser). Dado un elemento $a \in R$ tenemos que

$$f(a) = \bar{f}_s \circ i(a) = \bar{f}_s(a + 0X + 0X^2 + \cdots)$$

y por hipótesis $f(X) = s$. Por tanto, dado un polinomio $p(x) = a_0 + a_1x + \cdots + a_nX^n$ tenemos que

$$\begin{aligned}\bar{f}_s(p(x)) &= \bar{f}_s(a_0 + a_1x + \cdots + a_nX^n) = \bar{f}_s(a_0) + \bar{f}_s(a_1x) + \cdots + \bar{f}_s(a_nX^n)\\ &= \bar{f}_s(a_0) + \bar{f}_s(a_1)\bar{f}_s(x) + \cdots + \bar{f}_s(a_n)\bar{f}_s(X)^n = f(a_0) + f(a_1)s + \cdots + f(a_n)s^n\end{aligned}$$

Esta igualdad nos esta diciendo cual es la única posibilidad que tenemos para definir $\bar{f}_s$. Por tanto ya hemos demostrado la unicidad. Demostremos ahora que esta definición de $\bar{f}_s$ verifica lo que dice el teorema: Por construcción $\bar{f}_s$ hace conmutativo el diagrama y $\bar{f}_s(x) = s$ por tanto sólo tenemos que demostrar que es un homomorfismo de anillos.

Sean $p(x) = a_0 + a_1x + \cdots + a_nX^n$ y $q(x) = b_0 + b_1x + \cdots + b_nX^n$ (puedo representarlos "con el mismo grado" completando el de grado menor con ceros) dos polinomios de $R[X]$. Entonces

$$\begin{aligned}\bar{f}_s(p(x) + q(x)) &= \bar{f}_s(a_0 + a_1x + \cdots + a_nX^n + b_0 + b_1x + \cdots + b_nX^n)\\ &= \bar{f}_s(a_0 + b_0 + (a_1 + b_1)x + \cdots + (a_n + b_n)X^n)\\ &= f(a_0 + b_0) + f(a_1 + b_1)s + \cdots + f(a_n + b_n)s^n)\\ &= f(a_0) + f(a_1)s + \cdots + f(a_n)s^n + f(b_0) + f(b_1)s + \cdots + f(b_n)s^n\\ &= \bar{f}_s(p(x)) + \bar{f}_s(q(x))\\ \bar{f}_s(p(x) \cdot q(x)) &= \bar{f}_s(a_0 + a_1x + \cdots + a_nX^n) \cdot (b_0 + b_1x + \cdots + b_nX^n))\\ &= \bar{f}_s(\sum_{i=0}^{2n}\left(\sum_{j=0}^{i} a_j \cdot b_{i-j}\right)X^i) = \sum_{i=0}^{2n}\left(\sum_{j=0}^{i} f(a_j \cdot b_{i-j})\right)s^i\\ &= \sum_{i=0}^{2n}\left(\sum_{j=0}^{i} f(a_j) \cdot f(b_{i-j})\right)s^i\\ &=^{\star} (f(a_0) + f(a_1)s + \cdots + f(a_n)s^n) \cdot (f(b_0) + f(b_1)s + \cdots + f(b_n)s^n)\\ &= \bar{f}_s(p(x)) \cdot \bar{f}_s(xq(x))\end{aligned}$$

Observar que el paso que está marcado con $\star$ es cierto al ser R un anillo conmutativo. Por tanto, $\bar{f}_s$ es un homomorfismo de anillo, lo que demuestra el teorema. ■

Definición 20 Sea R un anillo conmutativo y sea $R[X]$ el anillo de polinomios con coeficientes en R. Dado $s \in R$ y $p(X) \in R[X]$ se define al evaluación de $p(X)$ en s y se representa por $p(s)$ como $\bar{i}_s(p(X))$.

Nota: Observar que tal como se demostró en la proposición anterior, si consideramos el polinomio $p(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$, y el elemento $s \in R$

$$p(s) := \bar{i}_s(p(X)) = a_0 + a_1s + \cdots + a_ns^n$$

★ Los ejercicios del 34 al 37 te pueden servir para saber si has asimilado los conceptos de esta sección.

Fin de clase 21; 22-11-2011, grupo A. Fin de clase 20; 22-11-2011, grupo B.

4.5. La unitización de un anillo

En la siguiente proposición vamos a demostrar que todo anillo se puede ver como subanillo de un anillo unitario:

Sea R un anillo y sea $\mathbb{Z}$ el anillo de los enteros. Entonces podemos definir una aplicación $\Phi : \mathbb{Z} \times R \to R$ definida por:

$$\Phi(n,z) = \begin{cases} z + z + \overset{n)}{\cdots} + z, & n > 0 \\ 0, & n = 0 \\ -z - z - \overset{-n)}{\cdots} - z, & n < 0. \end{cases}$$

Normalmente esta aplicación se denota simplemente por yuxtaposición, $\Phi(n,x) = nx$ y satisface las siguientes propiedades:

$$\begin{array}{cc} (n+m)x = nx + mx & n(x+y) = nx + ny \\ (nm)x = n(mx) & n(xy) = (nx)y = x(ny) \end{array}$$

Proposición 21 *Sea R un anillo. Entonces $\mathbb{Z} \times R$ con suma y producto:*

$$\begin{aligned} (\lambda, r) + (\mu, r') &:= (\lambda + \mu, r + r') \\ (\lambda, r).(\mu, r') &:= (\lambda\mu, \lambda r' + \mu r + r.r') \end{aligned}$$

Tiene estructura de anillo unitario. Es más, la aplicación $\psi : R \to \mathbb{Z} \times R$ dada por $\psi(r) = (0, r)$ es un monomorfismo de anillos.

Definición 22 Sea R un anillo. Se define la unitización de R, y se representa por R^1 como R, si éste ya es un anillo unitario o $\mathbb{Z} \times R$ caso de que R no sea unitario.

5. La característica de un anillo

Definición 1 Sea R un anillo. Si existe el menor natural $n \in \mathbb{N}$ tal que $a + \overset{n)}{\cdots} + a = 0$ para todo $a \in R$ se dice que la característica de R es n. En caso contrario se dice que la característica de R es cero.

Ejemplos A *Dado $n \in \mathbb{N}$, la característica de $\mathbb{Z}_n$ es n. La característica de $\mathbb{Z}$ es cero.*

Proposición 2 Sea R un anillo unitario. Entonces la característica de R o es cero o el menor natural tal que $1 + \overset{n)}{\cdots} + 1 = 0$ (o excluyente).

Demo: Si no existe ningún $k \in \mathbb{N}$ tal que $1 + \overset{k)}{\cdots} + 1 = 0$, entonces, por definición, la característica de R es cero. Supongamos que existe un $k \in \mathbb{N}$ tal que $1 + \overset{k)}{\cdots} + 1 = 0$ y sea n el menos natural que cumple esta propiedad. entonces, para todo $a \in R$,

$$a + \overset{k)}{\cdots} + a = a1 + \overset{k)}{\cdots} + a1 = a(1 + \overset{k)}{\cdots} + 1) = a0 = 0$$

Por lo que n es la característica de R. ■

Proposición 3 (ejercicio) La característica de un anillo y de su unitización no tienen que coincidir. Es más, si R no es unitario la característica de R^1 es cero.

Proposición 4 (ejercicio) ¿Se te ocurre una nueva construcción para "sumergir" un anillo no unitario en un anillo unitario manteniendo la característica?

Proposición 5 La característica de un dominio de integridad D es cero o un número primo.

Demo: Si la característica de D es cero no hay nada que demostrar. Supongamos por tanto que D tiene característica $n \in \mathbb{N}$. Por reducción al absurdo, si n no fuera primo, existiría $r, s \in \mathbb{N}$, con $1 < r, s < n$ tales que $n = rs$. En este caso,

$$0 = 1 + \overset{n)}{\cdots} + 1 = (1 + \overset{r)}{\cdots} + 1)(1 + \overset{s)}{\cdots} + 1).$$

Lo que implicaría, al ser n el menor natural con $1 + \overset{n)}{\cdots} + 1 = 0$ que $1 + \overset{r)}{\cdots} + 1$ y $1 + \overset{s)}{\cdots} + 1$ son dos elementos no nulos de D de producto cero, una contradicción ya que en D no hay divisores de cero. ■

★ Los ejercicios del 38 al 42 te pueden servir para saber si has asimilado los conceptos de esta sección.

Fin de clase 22; 24-11-2011, grupo A. Fin de clase 21; 24-11-2011, grupo B.

6. Los Cuaterniones de Hamilton

Hasta ahora no hemos visto un anillo de división que no sea conmutativo, es decir, un anillo de división que no sea cuerpo. Veamos aquí el primero.

La construcción del anillo de los cuaterniones de Hamilton es muy parecida a como se construye $\mathbb{C}$, los números complejos, a partir de $\mathbb{R}$, el cuerpo de los reales:

Vamos a considerar como conjunto base $\mathbb{H} := \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Denotamos los siguientes elementos como:

$$1 := (1, 0, 0, 0) \qquad i := (0, 1, 0, 0)$$
$$j := (0, 0, 1, 0) \qquad k := (0, 0, 0, 1)$$

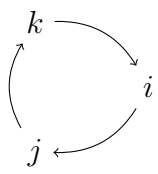
Con esta notación tenemos que los elementos de $\mathbb{H}$ son de la forma

$$\mathbb{H} := \{\alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k \ | \alpha_i \in \mathbb{R}, i = 1, \ldots, 4\}.$$

En este conjunto definimos la suma por componentes, con lo que $(\mathbb{H}, *)$ tiene estructura de grupo abeliano (es una mera comprobación). Definimos el producto en $\mathbb{H}$ siguiendo las siguientes reglas:

$$i^2 = -1 \quad j^2 = -1 \quad k^2 = -1 \quad 1 \cdot h = h \cdot 1 \ \forall h \in \mathbb{H} \quad \text{y}$$

Si multiplicas dos de estos siguiendo la dirección de las flechas te da el siguiente, $i \cdot j = k \quad j \cdot k = i \quad k \cdot i = j$. Si multiplicas dos de estos en sentido contrario a las flechas te da el siguiente cambiado de signo, $j \cdot i = -k \quad k \cdot j = -i \quad i \cdot k = -j$.



Todos los demás productos aparecen aplicado la propiedad distributiva:

$$\begin{aligned}(\alpha_1+\alpha_2 i+\alpha_3 j+\alpha_4 k)\cdot(\beta_1+\beta_2 i+\beta_3 j+\beta_4 k) :&= \alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3-\alpha_4\beta_4\\ &+(\alpha_1\beta_2+\alpha_2\beta_1+\alpha_3\beta_4-\alpha_4\beta_3)i\\ &+(\alpha_1\beta_3-\alpha_2\beta_4+\alpha_3\beta_1+\alpha_4\beta_2)j\\ &+(\alpha_1\beta_4+\alpha_2\beta_3-\alpha_3\beta_2+\alpha_4\beta_1)k\end{aligned}$$

Teorema 1 Con las notaciones anteriores, $(\mathbb{H},+,\cdot)$ es un anillo de división no conmutativo (por tanto no es un cuerpo).

Demo: El principio de la demostración de la proposición 1 (Pag. 63) nos demuestra que $(\mathbb{H},+)$ es un grupo abeliano, por lo que sólo nos tenemos que preocupar de demostrar las demás propiedades:

$\star$ La asociatividad del producto: Denotemos por $p_1=1, p_2=i, p_3=j, p_4=k$. Tenemos entonces

$$\left((\sum_{r=1}^{4}\alpha_i p_i)(\sum_{s=1}^{4}\beta_i p_i)\right)(\sum_{t=1}^{4}\gamma_i p_i)=\sum_{r,s,t=1}^{4}\alpha_r\beta_s\gamma_t\,(p_rp_s)p_t$$

$$(\sum_{r=1}^{4}\alpha_i p_i)\left((\sum_{s=1}^{4}\beta_i p_i)(\sum_{t=1}^{4}\gamma_i p_i)\right)=\sum_{r,s,t=1}^{4}\alpha_r\beta_s\gamma_t\,p_r(p_sp_t)$$

Luego, si para todo $r,s,t\in\{1,2,3,4\}$, $(p_rp_s)p_t=p_r(p_sp_t)$, entonces los dos sumatorios anteriores serán iguales y habremos demostrado la propiedad asociativa.

(a). Si $r=1$ o $s=1$ o $t=1$, entonces $(p_1p_s)p_t=p_sp_t=p_1(p_sp_t)$.

(b). Si $r=s=k$, $(p_rp_r)p_r=-p^r=p_r(p_rp_r)$. Veamos las siguientes 24 igualdades restantes:

$(ii)j=-j=ik=i(ij)$	$(ij)i=ki=j=-ik=i(ji)$	$(ji)i=-ki=-j=j(ii)$
$(ii)k=-k=-ij=i(ik)$	$(ik)i=-ji=k=ij=i(ki)$	$(ki)i=ji=-k=k(ii)$
$(jj)k=-k=ji=j(jk)$	$(jk)j=ij=k=-ji=j(kj)$	$(kj)j=-ij=-k=k(jj)$
$(jj)i=-i=-jk=j(ji)$	$(ji)j=-kj=i=jk=j(ij)$	$(ij)j=kj=-i=i(jj)$
$(kk)i=-i=kj=k(ki)$	$(ki)k=jk=i=-kj=k(ik)$	$(ik)k=-jk=-i=i(kk)$
$(kk)j=-j=-ki=k(kj)$	$(kj)k=-ik=j=ki=k(jk)$	$(jk)k=ik=-j=j(kk)$
$(ij)k=k^2=i^2=i(jk)$	$(ji)k=-k^2=-j^2=j(ik)$	$(ik)j=-j^2=-i^2=i(kj)$
$(ki)j=j^2=k^2=k(ij)$	$(jk)i=i^2=j^2=j(ki)$	$(kj)i=-i^2=-k^2=k(ji)$

$\star$ Es claro que $(\mathbb{H},+,\cdot)$ es unitario, con unidad 1.

$\star$ Es claro que $(\mathbb{H},+,\cdot)$ no es conmutativo, ya que $ij=k$, y $ji=-k$.

$\star$ Tenemos que demostrar ahora que todo elemento no nulo de $(\mathbb{H},+,\cdot)$ posee un inverso. Pero,

$$(\alpha_1+\alpha_2 i+\alpha_3 j+\alpha_4 k)\cdot(\alpha_1-\alpha_2 i-\alpha_3 j-\alpha_4 k)=\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2$$

por tanto, si $h=\alpha_1+\alpha_2 i+\alpha_3 j+\alpha_4 k\neq 0$, $0\neq\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2\in\mathbb{R}$ y

$$h^{-1}=\frac{\alpha_1}{\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2}-\frac{\alpha_2}{\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2}i-\frac{\alpha_3}{\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2}j-\frac{\alpha_4}{\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2}k$$

Lo que demuestra que todo elemento no nulo de $\mathbb{H}$ posee inverso.

$\star$ Por último la distributiva es evidente, por la propia definición del producto. ■

Definición 2 *Sea* $(\mathbb{H}, +, \cdot)$ *el anillo de división de los Cuaterniones de Hamilton. Se define:*

- *El conjugado de un elemento* $h = \alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k \in \mathbb{H}$ *y se denota por* $\overline{h}$ *como* $\overline{h} := \alpha_1 - \alpha_2 i - \alpha_3 j - \alpha_4 k$.
- *Se define la norma de un elemento* $h = \alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k \in \mathbb{H}$ *y se denota por* $|h|$ *como* $|h| := \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$.

Nota: Observar que el inverso de un elemento no nulo $h \in \mathbb{H}$ es $h^{-1} = \frac{\overline{h}}{|h|}$.

7. Ampliación de contenidos

7.1. Anillos de endomorfismos de un grupo abeliano

Nota: El conjunto de los homomorfismos entre dos anillos R y R' no tiene muy buenas propiedades, ya que ni la suma natural de aplicaciones es un homomorfismo: si consideramos la identidad en $\mathbb{Z}$, el anillo de los enteros, se tiene que $Id + Id$ no es un homomorfismo. ¿Cuales son los endomorfismos de $\mathbb{Z}$?

Definición 1 *Sean* G *y* G' *dos grupos. Se define un* ***homomorfismo de grupos*** *de* G *en* G' *como una aplicación* $f : G \to G'$ *tal que:*

$$f(a + b) = f(a) +' f(b) \quad \text{para todo } a, b \in G$$

Se define $\mathrm{Hom}(G, G')$ *como el conjunto de todos los homomorfismos de* G *en* G'. *Por* $\mathrm{End}(G)$ *denotaremos al conjunto de todos los homomorfismos de* G *en* G.

Proposición 2 *Sean* G *y* G' *dos grupos. Entonces*

(1) $\mathrm{Hom}(G, G')$ *es un grupo con la suma usual: dados* $f, g \in \mathrm{Hom}(G, G')$,

$$f + g : G \to G' \quad \text{definida por} \quad f + g(a) = f(a) + g(a).$$

Es mas, si G' *es conmutativo,* $\mathrm{Hom}(G, G')$ *es un grupo abeliano*

(2) $\mathrm{End}(G)$ *con la suma usual y la composición de aplicaciones,* $(\mathrm{End}(G), +, \circ)$ *es un anillo unitario.*

Teorema 3 *Todo anillo es isomorfo a un subanillo de un anillo de endomorfismos de un cierto grupo abeliano.*

Demo: Consideremos R^1 con su estructura de grupo abeliano. Veamos que la aplicación $\Phi : R \to \mathrm{End}(R^1)$ definida por $\Phi_r(r') = rr'$ es un monomorfismos de anillos: dados r_1 y r_2 elementos de R,

– $\Phi_{r_1+r_2}(r') = (r_1 + r_2)r' = r_1 r' + r_2 r' = \Phi_{r_1}(r') + \Phi_{r_2}(r')$

– $\Phi_{r_1}\Phi_{r_2}(r') = r_1(r_2 r') = (r_1 r_2)r' = \Phi_{r_1 r_2}(r')$

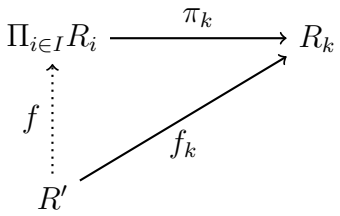
Lo que demuestra que es un homomorfismo de anillos. Por último, si $\Phi_r = 0$, $0 = \Phi_r(1) = r$, lo que demuestra que es inyectiva. ■

Nota: Este teorema nos dice como son todos los anillos (resultado poco útil).

Nota: La aplicación inversa de un automorfismo $f : R \to R$ es precisamente el inverso de f en $\mathrm{End}(R)$ (considerado R únicamente como grupo abeliano).

7.2. Propiedad fundamental del producto directo de anillos

Proposición 4 *Sean R_i, $i \in I$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los R_i. Entonces para cada anillo R' y cada familia de homomorfismos de anillos $f_i : R' \to R_i$ existe un único homomorfismo de anillos $f : R' \to R$ tal que para cada $k \in I$ el siguiente diagrama es conmutativo:*



Es más, Si $\hat{R}$ es un anillo y $\rho_i : \hat{R} \to R_i$ son una familia de epimorfismos de anillos tales que para cada anillo R' y cada familia de homomorfismos de anillos $f_i : R' \to R_i$ existe un único homomorfismo de anillos $f : R' \to \hat{R}$ tal que para cada $k \in I$ el diagrama anterior es conmutativo, entonces $\hat{R}$ es isomorfo a $\Pi_{i\in I} R_i$.

Demo: Tenemos que demostrar la existencia y unicidad del homomorfismo $f : R' \to R$ que hace conmutativo el diagrama. La estrategia que vamos a usar para demostrarlo va a consistir en demostrar que hay una única aplicación que hace conmutativo el diagrama y para luego demostrar que esta única posibilidad es el homomorfismo de anillos que buscamos:

1-. Supongamos que existe $f : R' \to \Pi_{i\in I} R_i$ tales que $\pi_k \circ f = f_k$ tenemos entonces que dado $r' \in R'$, $f_k(r') = \pi_k(f(r'))$, por lo que la coordenada k-esima de $f(r')$ es $f_k(r')$. Así, $f(r')$ tiene que ser forzosamente $(f_i(r'))_{i\in I}$.

2-. Comprobemos entonces que la aplicación $f : R' \to \Pi_{i\in I} R_i$ definido por $f(r') = (f_i(r'))_{i\in I}$ es un homomorfismo de anillos que verifica el enunciado:

$\star$ ¿Es homomorfismo de grupos?

$$\begin{aligned} f(r'_1 + r'_2) &= (f_i(r'_1 + r'_2))_{i\in I} = (f_i(r'_1) + f_i(r'_2))_{i\in I} = (f_i(r'_1))_{i\in I} + (f_i(r'_2))_{i\in I} \\ &= f(r'_1) + f(r'_2) \end{aligned}$$

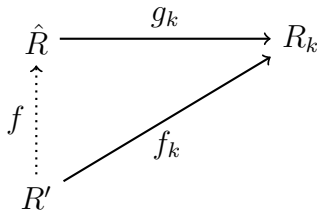
$\star$ ¿Es homomorfismo de anillos?

$$\begin{aligned} f(r'_1.r'_2) &= (f_i(r'_1.r'_2))_{i\in I} = (f_i(r'_1).f_i(r'_2))_{i\in I} = (f_i(r'_1))_{i\in I}.(f_i(r'_2))_{i\in I} \\ &= f(r'_1)f(r'_2) \end{aligned}$$

$\star$ ¿Hace conmutativo los diagramas? Pues claro

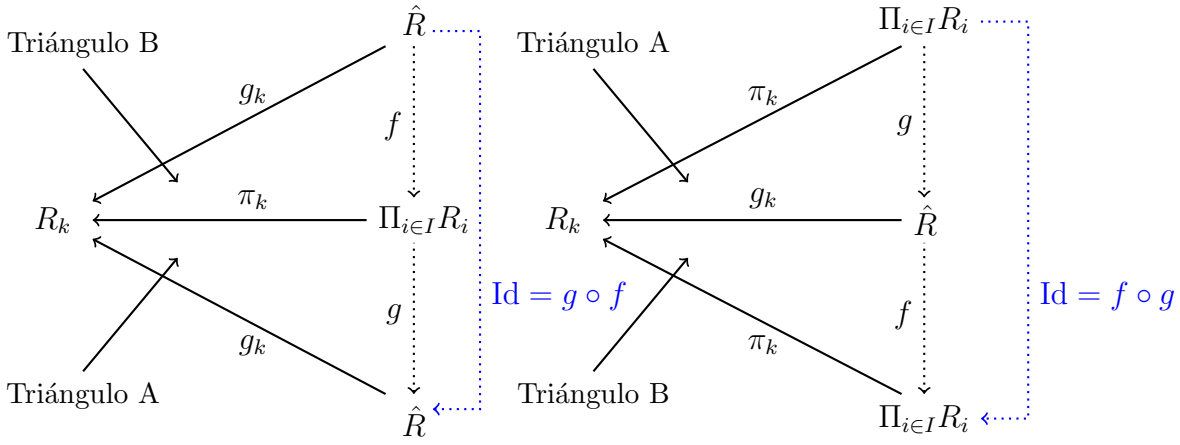
$$\pi_k \circ f(r') = \pi_k((f_i(r'))_{i\in I})) = f_k(r').$$

Veamos ahora que todo anillo con estas propiedades es isomorfo al producto cartesiano de los $\{R_i\}_{i\in I}$. Sea $\hat{R}$ un anillo y $g_i : \hat{R} \to R_i$ una familia de epimorfismos de anillos tales que para cada anillo R' y cada familia de homomorfismos de anillos $f_i : R' \to R_i$ existe un único homomorfismo de anillos $f : R' \to \hat{R}$ tal que para cada $k \in I$ el diagrama



es conmutativo.

Si consideramos ahora $R' = \Pi_{i\in I} R_i$ y $f_i = \pi_i$ las proyecciones canónicas tenemos:



En donde f es la única aplicación que hace conmutativo el triángulo B (aquí estamos aplicando que $\Pi_{i\in I} R_i$ verifica la propiedad del producto cartesiano, apartado 1-.) y en donde g es la única aplicación que hace conmutativo el triángulo A (aquí estamos aplicando que, por hipótesis, $\hat{R}$ satisface la propiedad). Ahora,

$$g_k \circ \mathrm{Id} = g_k = \pi_k \circ g = (g_k \circ f) \circ g = g_k \circ (f \circ g)$$

Luego como $\hat{R}$ verifica la propiedad, $\mathrm{Id}_{\hat{R}} = f \circ g$ (estamos haciendo uso de la unicidad de la solución). Pero igualmente, si nos fijamos en el exterior del segundo diagrama,

$$\pi_k \circ \mathrm{Id} = \pi_k = g_k \circ f = (\pi_k \circ g) \circ f = \pi_k \circ (g \circ f)$$

Luego como $\Pi_{i\in I} R_i$ verifica la propiedad, $\mathrm{Id}_{\Pi_{i\in I} R_i} = g \circ f$ (estamos haciendo uso de la unicidad de la solución). Por tanto f y g son isomorfismo de anillos lo que demuestra que $\Pi_{i\in I} R_i$ y $\hat{R}$ son isomorfos. ■

7.3. Asociatividad en el producto de matrices

$$\left[\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}\right] \cdot \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} =$$

$$\begin{pmatrix} \sum_{r=1}^{n} a_{1r} \cdot b_{r1} & \sum_{r=1}^{n} a_{1r} \cdot b_{r2} & \cdots & \sum_{r=1}^{n} a_{1r} \cdot b_{rn} \\ \sum_{r=1}^{n} a_{2r} \cdot b_{r1} & \sum_{r=1}^{n} a_{2r} \cdot b_{r2} & \cdots & \sum_{r=1}^{n} a_{2r} \cdot b_{rn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{r=1}^{n} a_{nr} \cdot b_{r1} & \sum_{r=1}^{n} a_{nr} \cdot b_{r2} & \cdots & \sum_{r=1}^{n} a_{nr} \cdot b_{rn} \end{pmatrix} \cdot \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} =$$

$$\begin{pmatrix} \sum_{r,s=1}^{n} (a_{1r} \cdot b_{rs}) \cdot c_{s1} & \sum_{r,s=1}^{n} (a_{1r} \cdot b_{rs}) \cdot c_{s2} & \cdots & \sum_{r,s=1}^{n} a_{1r} \cdot b_{rs}) \cdot c_{sn} \\ \sum_{r,s=1}^{n} (a_{2r} \cdot b_{rs}) \cdot c_{s1} & \sum_{r,s=1}^{n} (a_{2r} \cdot b_{rs}) \cdot c_{s2} & \cdots & \sum_{r,s=1}^{n} (a_{2r} \cdot b_{rs}) \cdot c_{sn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{r,s=1}^{n} (a_{nr} \cdot b_{rs}) \cdot c_{s1} & \sum_{r,s=1}^{n} (a_{nr} \cdot b_{rs}) \cdot c_{s2} & \cdots & \sum_{r,s=1}^{n} (a_{nr} \cdot b_{rs}) \cdot c_{sn} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \left[\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} \cdot \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix}\right] =$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} \sum_{s=1}^{n} b_{1s} \cdot c_{s1} & \sum_{s=1}^{n} b_{1s} \cdot c_{s2} & \cdots & \sum_{s=1}^{n} b_{1s} \cdot c_{sn} \\ \sum_{s=1}^{n} b_{2s} \cdot c_{s1} & \sum_{s=1}^{n} b_{2s} \cdot c_{s2} & \cdots & \sum_{s=1}^{n} b_{2s} \cdot c_{sn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{s=1}^{n} b_{ns} \cdot c_{s1} & \sum_{s=1}^{n} b_{ns} \cdot c_{s2} & \cdots & \sum_{s=1}^{n} b_{ns} \cdot c_{sn} \end{pmatrix} =$$

$$\begin{pmatrix} \sum_{r,s=1}^{n} a_{1r} \cdot (b_{rs} \cdot c_{s1}) & \sum_{r,s=1}^{n} a_{1r} \cdot (b_{rs} \cdot c_{s2}) & \cdots & \sum_{r,s=1}^{n} a_{1r} \cdot (b_{rs} \cdot c_{sn}) \\ \sum_{r,s=1}^{n} a_{2r} \cdot (b_{rs} \cdot c_{s1}) & \sum_{r,s=1}^{n} a_{2r} \cdot (b_{rs} \cdot c_{s2}) & \cdots & \sum_{r,s=1}^{n} a_{2r} \cdot (b_{rs} \cdot c_{sn}) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{r,s=1}^{n} a_{nr} \cdot (b_{rs} \cdot c_{s1}) & \sum_{r,s=1}^{n} a_{nr} \cdot (b_{rs} \cdot c_{s2}) & \cdots & \sum_{r,s=1}^{n} a_{nr} \cdot (b_{rs} \cdot c_{sn}) \end{pmatrix}$$

8. Ejercicios del Tema

1 Decir si los siguientes conjuntos, con las operaciones indicadas, tienen estructura de anillo. En caso afirmativo: ¿son conmutativos?, ¿unitarios?, ¿de división?... ¿cuáles son sus elementos inversibles?

(i) $\mathbb{Z}^+$ con la suma y producto usual.

(ii) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ con la suma y producto usual.

(iii) $\mathbb{N}$ con primera operación: el producto y segunda operación la potencia, es decir:
"$a + b$ igual a ab" y "a por b igual a a^b".

(iv) $\{x \in \mathbb{Q} \mid 3x \in \mathbb{Z}\}$ con las operaciones usuales.

2 Sea X un conjunto no vacío, $\mathcal{P}$ el conjunto de partes de X y $\triangle$ la operación diferencia simétrica. Demuestra que $(\mathcal{P}(X), \triangle, \cap)$ es un anillo conmutativo y unitario. Da una condición necesaria y suficiente para que sea dominio de integridad.

3 Sea $(R, +, \cdot)$ un anillo y sea $a \in R$. Demuestra que R con su misma suma y un nuevo producto dado por $x \cdot_a y = xay$ tiene estructura de anillo, es decir, que $(R, +, \cdot_a)$ tiene estructura de anillo. ¿Se te ocurre alguna condición para que este nuevo anillo sea unitario?

4 Sea R un anillo unitario y sea $\mathcal{U}(R)$ el conjunto de los elementos inversibles de R. Demuestra que el producto de R define una operación en $\mathcal{U}(R)$ que dota a éste de estructura de grupo. Demuestra que si R es un anillo conmutativo, $(\mathcal{U}(R), \cdot)$ es un grupo abeliano.

5 Sea R un anillo. Demuestra que si $a \in R$ es un divisor de cero, entonces a no es inversible.

6 ¿Puedes encontrar un anillo R con divisores de cero por la izquierda pero sin divisores de cero por la derecha?

7 Sea $(R, +, \cdot)$ un anillo. Demuestra que las siguientes condiciones son equivalentes:

(i) R no posee divisores de cero por la izquierda (Resp. derecha).

(ii) Se verifican las leyes de cancelación por la izquierda (Resp. derecha).

8 Demuestra que para un anillo conmutativo y unitario $(R, +, \cdot)$ las siguientes condiciones son equivalentes:

(i) R es un dominio de integridad.

(ii) Se verifican las leyes de cancelación en R. Es decir,

$$\text{Si } ax = ay \text{ con } a \neq 0, \text{ entonces } x = y$$
$$\text{Si } xa = ya \text{ con } a \neq 0, \text{ entonces } x = y$$

9 Sea $(R, +, \cdot)$ un anillo. Demuestra que R verifica la ley de cancelación por la izquierda si y sólo si verifica la ley de cancelación por la derecha.

10 Demuestra que en un anillo unitario $(R, +, \cdot)$ el cero (neutro para la suma) y el 1 (neutro para el producto) son elementos distintos.

11 ¿Es posible dar una estructura de anillo en el conjunto $\mathbb{Z}$ en donde la primera operación sea el producto? ¿Y en la que la segunda operación sea la suma? Demuestra que no es posible o construye dicha operación. *

12 Sea R un anillo unitario y $a \in R$ tal que existe $b \in R$ con $ab = 1$. Demuestra que son equivalentes: *

- a no es inversible.
- existe $b' \in R$ con $b' \neq b$ y $ab' = 1$.
- a es divisor de cero.

Demuestra que en las condiciones anteriores, R contiene un idempotente no trivial (distinto de 0 y 1). *

13 Sea R un anillo. Demuestra que si para todo $a, b \in R$ la ecuación $aX = b$ tiene a lo sumo una solución, entonces en R no hay divisores de cero. ¿Es cierto del recíproco? *

14 Demuestra que en $\mathbb{Z}_{12}$ la ecuación $X^2 - 1 = 0$ tiene más de dos soluciones. Demuestra que en un dominio de integridad la ecuación anterior sólo posee, a lo sumo, dos soluciones. ¿Sabrías encontrar un anillo en donde sólo posea una?

15 Sea R un anillo. Un elemento $x \in R$ se dice idempotente si $x = x^2$. Demuestra que un anillo en donde todo elemento es idempotente es conmutativo. *

16 Sea R un anillo y $e \in R$ un idempotente. Demuestra que

$$eRe := \{exe \mid x \in R\} = \{x \in R \mid xe = ex = x\}$$

es un subanillo unitario de R (que no se te olvide comprobar la igualdad de los conjuntos anteriores). Demuestra que si $eRe = R$, entonces $e = 1$.

17 Demuestra que todo subanillo unitario de un dominio de integridad es un dominio de integridad. En particular, todo subanillo unitario de un cuerpo es un dominio de integridad.

18 Demuestra que si R es un anillo unitario y S es un subanillo suyo, S no tiene por qué ser unitario. Es más, si S es unitario las unidades de R y S pueden no coincidir. *

19 Sea R un anillo sin divisores de cero y S un subanillo de R. Demuestra que si S es unitario, entonces R es unitario con la misma unidad.

20 Sea R un anillo y $f : R \to \mathcal{M}_2(R)$ definido por $f(r) = \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$. Demuestra que f es un monomorfismo de anillos.

21 Sean $n, m \in \mathbb{N}$ primos entre si. Demuestra que la aplicación $f : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ definida por $f(\overline{r}) = (\overline{r}, \overline{r})$ es un isomorfismo de anillos. (Acuérdate de demostrar que f está bien definida)

22 Sea R un anillo y $f : R \to R$ un homomorfismo de anillos. Demuestra que la aplicación $\hat{f} : \mathcal{M}_2(R) \to \mathcal{M}_2(R)$ definido por $\hat{f}(a_{ij}) = (f(a_{ij}))$ es un homomorfismo de anillos. Demuestra que si f es un monomorfismo $\hat{f}$ también lo es. ¿Si f es un epimorfismo, $\hat{f}$ tiene que serlo?

23 Encuentra un homomorfismo $f : R \to R'$ con R y R' anillos unitarios y $f(1_R) \neq 1_{R'}$.

24 ¿Cuales son los endomorfismos de $\mathbb{Z}$?

25 Sea R un anillo. Encuentra dos monomorfismo de anillos $f : R \to \mathcal{M}_2(R)$.

26 Se dice que una propiedad (que pueda poseer un anillo) es estructural si siempre que la verifique un anillo R la verifica cualquier anillo isomorfo a él (R y R' son isomorfos si existe un isomorfismo $f : R \to R'$). Demuestra que ser conmutativo, ser unitario, no poseer divisores de cero, poseer n elementos inversibles son propiedades estructurales. ¿Se te ocurre alguna más?

27 Demuestra que no hay ningún isomorfismo entre $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$.

28 Sean R y R' dos anillos y $f : R \to R'$ un homomorfismo de anillos. Entonces:

(i) Si R es un anillo unitario, $\mathrm{Im}(f)$ es un anillo unitario con unidad $f(1)$.
(ii) Si a es un elemento inversible de R, $f(a)$ es un elemento inversible de $\mathrm{Im}(f)$.
(iii) Si f es sobreyectiva, entonces $f(1) = 1'$ y $f(a)$ es inversible para todo elemento inversible $a \in R$.
(iv) Si R y R' son unitarios y $f(1) = 1'$, $f(a)$ es inversible para todo elemento inversible $a \in R$.

29 *Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los R_i. Demuestra que para cada $k \in I$, la proyección canónica $\pi_k : \Pi_{i\in I} R_i \to R_k$ es un epimorfismo de anillos.*

30 *Sean $\{R_i\}_{i\in I}$, $\{S_i\}_{i\in I}$ dos familia de anillos indizadas en el mismo conjunto I. Supongamos que para cada $i \in I$ existe un homomorfismo de anillos $f_i : R_i \to S_i$. Demuestra que existe un único homomorfismo de anillos $f : \{R_i\}_{i\in I} \to \{S_i\}_{i\in I}$ tal que $f_i \circ \pi_i^r = \pi_i^s \circ f$.*

31 *Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los R_i. Demuestra que,*

- *R es unitario si y sólo si R_k es unitario para todo $k \in I$.*
- *R es conmutativo si y sólo si R_k es conmutativo para todo $k \in I$.*
- *Si $\#I \geq 2$, R tiene divisores de cero. Por tanto, en este caso, R no puede ser dominio de integridad, anillo de división o cuerpo.*

32 *Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \bigoplus_{i\in I} R_i$ la suma directa de los R_i. Demuestra que para cada $k \in I$, la inclusión canónica $\rho_k : R_k \to \bigoplus_{i\in I} R_i$ es un monomorfismo de anillos.*

33 *Sea R un anillo y $n \in \mathbb{N}$. Demuestra los siguientes enunciados:*

(i) $\mathcal{M}_n(R)$ *es unitario si y sólo si* R *es unitario.*
(i) $\mathcal{M}_n(R)$ *tiene divisores de cero si* $n \leq 2$*. Por tanto, en este caso,* $\mathcal{M}_n(R)$ *no puede ser dominio de integridad, anillo de división o cuerpo.*
(ii) $\mathcal{M}_n(R)$ *es conmutativo si y sólo si* R *es conmutativo y* $n = 1$*.*
(iii) $\mathcal{M}_n(R)$ *es un anillo de división si y sólo si* R *es un anillo de división y* $n = 1$*.*
(iv) $\mathcal{M}_n(R)$ *es un cuerpo si y sólo si* R *es un cuerpo y* $n = 1$*.*

34 *Sea* R *un anillo y sea* $R[[X]]$ *el anillo de series formales con coeficientes en* R*. Entonces:*

(i) R *es unitario si y sólo si* $R[[X]]$ *es unitario.*
(ii) R *es conmutativo si y sólo si* $R[[X]]$ *es conmutativo.*
(ii) R *es D.I si y sólo si* $R[[X]]$ *es D.I.*

35 *Sea* R *un anillo unitario y sea* $R[[X]]$ *el anillo de series formales con coeficientes en* R*. Entonces un elemento* $\sum_{n=0}^{\infty} a_n X^n \in R[[X]]$ *es inversible si y sólo si* a_0 *es un elemento inversible de* R*.*

36 *Sea* R *un anillo unitario y sea* $R[[X]]$ *el anillo de series formales con coeficientes en* R*.Calcula el inverso de la serie* $p(x) = 1 - x$*.*

37 Sea R un anillo y sea $R[X]$ el anillo de polinomios con coeficientes en R y sean $p(X), q(X) \in R[X]$. Entonces

(i) R es conmutativo si y sólo si $R[X]$ es conmutativo.
(ii) R es unitario si y sólo si $R[X]$ es unitario.
(iii) R es dominio de integridad si y sólo si $R[X]$ es dominio de integridad.
(iv) $\deg(p(X) + q(X)) \leq \text{Max}(\deg(p(X)), \deg(q(X)))$.
(v) $\deg(p(X) \cdot q(X)) \leq \deg(p(X)) + \deg(q(X))$.
(vi) Es más, R no posee divisores de cero si para todo $p(X), q(X) \in R[X]$ se tiene que

$$\deg(p(X) \cdot q(X)) = \deg(p(X)) + \deg(q(X)).$$

38 Sea R un anillo sin divisores de cero y sea R^1 su unitización. ¿Puede suceder que R^1 tenga divisores de cero?

39 Demuestra que la característica de un anillo y de su unitización no tienen que coincidir. Es más, si R no es unitario la característica de R^1 es cero.

40 ¿Se te ocurre una nueva construcción para "sumergir" un anillo no unitario en un anillo unitario manteniendo la característica? *

41 Sea R un anillo (no necesariamente unitario) de característica 6. Demuestra que en R hay divisores de cero.

42 Sea R un anillo de característica n y S un anillo de característica m. Determina la característica de los siguientes anillos:

(i) El anillo producto cartesiano, R^n
(ii) El anillo producto cartesiano, $R \times S$.
(iii) El anillo de polinomios, $R[X]$.
(iv) El anillo de matrices, $\mathcal{M}_k(R)$.

43 Sea $(M, *)$ un monoide. Demuestra que si existe $a \in M$, a distinto del neutro, con $a^2 = a$, entonces $(M, *)$ no es un grupo. *

44 *Sea $\mathbb{H}$ el anillo de los cuaterniones de Hamilton. Calcula la norma y el inverso de los siguientes elementos:*

$$1 + i + j + k, \quad 1 - i + j - k \quad 1 + i$$

45 *Sea $\mathbb{H}$ el anillo de los cuaterniones de Hamilton. Calcula todos los elementos x de $\mathbb{H}$ que verifiquen que $x^2 + 1 = 0$.*

46 Se dice que un elemento x en un anillo R es nilpotente si existe $n \in \mathbb{N}$, con $n > 1$, tal que $x^n = 0$. Encuentra una condición necesaria y suficiente para que $\mathbb{Z}_n$ no tenga elementos nilpotentes. Calcula los nilpotentes de $\mathbb{Z}_{120}$. *

47 Demuestra que un anillo R no posee elementos nilpotentes si y sólo si el único elemento $x \in R$ tal que $x^2 = 0$ es $x = 0$.

48 Demuestra que en un anillo sin divisores de cero los únicos (posibles) idempotentes son 0 y 1 (llamados idempotentes triviales). Encuentra algún idempotente no trivial en $\mathcal{M}_n(\mathbb{R})$.

49 Demuestra que en un anillo sin idempotentes no triviales, si $ab = 1$ entonces $ba = 1$.

50 Sea R un anillo con al menos dos elementos. Supongamos que para cada $0 \neq x \in R$ existe un **único** $y \in R$ con $x = xyx$. Demuestra que: R no tiene divisores de cero. Si $xyx = x$, entonces $yxy = y$. R es unitario. R es un anillo de división. **

51 Encuentra un anillo R que no sea de división y tal que para cada $x \in R$ exista $y \in R$ con $x = xyx$. *

52 ¿Puedes encontrar un anillo R y un elemento a tal que a sea divisor de cero por la derecha pero no sea divisor de cero por la izquierda? **

53 Da un ejemplo de un anillo R no conmutativo tal que el conjunto de sus elementos inversibles, $\mathcal{U}(R)$ sea un grupo abeliano y otro en el que sea un grupo no abeliano (con el producto de R). **

54 Sea $(M, *)$ un monoide. Demuestra que M es un grupo si para todo $a, b \in M$ la ecuación $a \cdot X = b$ tiene solución (es decir, existe $s \in M$ tal que $a \cdot s = b$. *

El símbolo [$*$] significa dificultad moderada y [$**$] dificultad media.

Capítulo 4

Cuerpo de fracciones de un dominio de integridad

Objetivos del capítulo

- En este tema vamos a estudiar mas en profundidad los dominios de integridad. Demostraremos que un anillo conmutativo y unitario es de integridad si y sólo si verifica las leyes de cancelación, lo que nos llevara a demostrar que todo dominio de integridad finito es cuerpo.
- Se recuerda la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$ y se generaliza para construir el cuerpo de fracciones de cualquier dominio de integridad. Como resultado particular se demuestra que un anillo es un dominio de integridad si y sólo si es subanillo de un cuerpo.
- Por último generalizaremos la construcción anterior para ciertos conjuntos de denominadores.

---

1. Caracterizaciones de un dominio de integridad

Definición 1 (Recordatorio) Sea R un anillo. Se dice que $0 \neq a \in R$ es:

- Un **divisor de cero por la izquierda** si existe $0 \neq b \in R$ tal que $a \cdot b = 0$.
- Un **divisor de cero por la derecha** si existe $0 \neq b \in R$ tal que $b \cdot a = 0$.

Nota: (Ejercicio) Si un anillo no tiene divisores de cero por la izquierda, entonces no tiene divisores de cero por la derecha.

Definición 2 (Recordatorio) Un anillo conmutativo y unitario sin divisores de cero se denomina un **dominio de integridad** (normalmente denotaremos los dominios de integridad por D.I.)

Definición 3 (Recordatorio) Recordamos que un anillo R verifica la **ley de cancelación por la izquierda** si dados $a, b, c \in R$ con $c \neq 0$, $ca = cb$ entonces $a = b$. Diremos que un anillo R verifica la **ley de cancelación por la derecha** si dados $a, b, c \in R$ con $c \neq 0$, $ac = bc$ entonces $a = b$.

Fin de clase 23; 25-11-2011, grupo A. Fin de clase 22; 25-11-2011, grupo B.

Fin de clase 23; 28-11-2011, grupo B. (recuperación clase 2 ejercicios)

Hecho en ejercicios

Proposición 4 (Ejercicio) Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R verifica la ley de cancelación por la izquierda.
(ii) R no tiene divisores de cero por la izquierda.
(iii) R no tiene divisores de cero por la derecha.
(iv) R verifica la ley de cancelación por la derecha.

Demo: $(i) \implies (ii)$. Supongamos que R verifica la ley de cancelación por la izquierda y sea $0 \neq a \in R$ tal que existe $b \in R$ con $ab = 0$. Tenemos entonces que $ab = 0 = a0$ y como R verifica la ley de cancelación por la izquierda $b = 0$ (luego en R no hay divisores de cero por la izquierda). $(iv) \implies (iii)$ es similar a esta demostración.

$(ii) \implies (iii)$. Supongamos que $0 \neq b$ es un divisor de cero por la derecha, entonces existe $0 \neq a \in R$ tal que $ab = 0$. pero entonces a es un divisor de cero por la izquierda (contradicción). $(iii) \implies (ii)$ es similar a esta demostración.

$(iii) \implies (iv)$. Supongamos que R no tiene divisores de cero por la derecha y sean $a, b, c \in R$, con $a \neq 0$ tales que $ba = ca$. Entonces $0 = ba - ca = (b - c)a$ y como en R no hay divisores de cero por la derecha, $b - c = 0$, es decir $b = c$. $(i) \implies (ii)$ es similar a esta demostración. ■

Nota: A partir de ahora hablaremos de anillos que verifican la ley de cancelación y anillos sin divisores de cero (ya no nos hace falta hablar de derecha o izquierda).

Nota: Todo dominio de integridad y todo anillo de división (en particular todo cuerpo) verifica la ley de cancelación.

Proposición 5 Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R no posee divisores de cero.
(ii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, la ecuación $aX + b = 0$ si poseen solución, ésta es única.
(iii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, la ecuación $Xa + b = 0$ si poseen solución, ésta es única.

Demo: $(i) \implies (ii)$. Supongamos que en R no hay divisores de cero y sean s, s' dos soluciones de la ecuación. Entonces $as + b = 0$ y $as' + b = 0$. Por tanto $as = -b = as'$ y como en R se verifica la ley de cancelación $s = s'$. $(i) \implies (iii)$ es similar.

$(ii) \implies (i)$. Supongamos que la ecuación $aX + b = 0$ de tener solución ésta es única. Por reducción al absurdo supongamos que R posee un divisor de cero. Entonces existen $a, b \in R$ no nulos tales que $ab = 0$ y por tanto la ecuación $aX = 0$ tiene dos soluciones $s = b$ y $s = 0$, contradicción. $(iii) \implies (i)$ es similar. ■

Proposición 6 Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R es un anillo de división.

(ii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, la ecuación $aX + b = 0$ poseen solución única.
(iii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, la ecuación $Xa + b = 0$ poseen solución única.

Demo: $(i) \implies (ii)$. Supongamos que R es un anillo de división y sea la ecuación $aX + b = 0$ con $a \neq 0$. Entonces, sea el elemento $s = -a^{-1}b$ que existe ya que R es un anillo de división y $a \neq 0$. Entonces $as + b = a(-a^{-1}b) + b = -b + b = 0$. Luego s es solución de la ecuación. Es más como en un anillo de división no hay divisores de cero, la solución es única. $(i) \implies (iii)$ es similar: es claro que la solución de la ecuación $Xa + b = 0$ es $s' = -ba^{-1}$ (que no tiene que coincidir con s, ya que R no tiene que ser conmutativo).

$(ii) \implies (i)$. En primer lugar demostremos que R es un anillo unitario (ya sabemos que no hay divisores de cero en R por la proposición 5 (Pag. 86)). Dado $0 \neq a \in R$ la ecuación $aX - a = 0$ posee una única solución. Sea $e \in R$ tal que $ae = a$.
Nota: sólo sabemos que $ae = a$ para cualquier otro elemento de $0 \neq b \in R$, el elemento be no sabemos que coincida con b. Planteando la ecuación $bX - b = 0$ sólo conseguiríamos un elemento e' tal que $be' = b$.

Como $ae = a$, si multiplicamos por e por la derecha tendríamos $ae^2 = ae$ y como no hay divisores de cero (por la izquierda) en R, $e^2 = e$ (es decir, e es un idempotente), no nulo de R, ya que si $e = 0$, $ae = 0$, una contradicción. Ahora, dado cualquier $x \in R$, $xe^2 = xe$ y aplicando la ley de simplificación $xe = x$. De forma similar $e^2x = ex$ y por tanto $ex = x$, es decir, e es elemento neutro del producto de R, por lo que R es unitario con unidad e (desde este momento al elemento e se denota por 1). Por último, solo tenemos que demostrar que todo elemento no nulo de R tiene inverso. Dado $0 \neq a \in R$, la ecuación $aX = 1$ posee solución, luego existe $s \in R$ tal que $as = 1$ (con lo que $s \neq 0$). Por tanto, la ecuación $sX = 1$ tiene solución (única) por lo que existe $b \in R$ con $sb = 1$. Ahora,

$$a = a1 = a(sb) = (as)b = 1b = b$$

lo que implica que s es el inverso de a en R. $(iii) \implies (i)$ es similar. ■

Nota: La siguiente noción es muy importante y se usara repetidamente a lo largo de la carrera.

Definición 7 • Sea R un anillo y sea $a \in R$ se define:

- la aplicación de **multiplicación por la izquierda de** a en R y se denota por $\lambda_a : R \to R$ como la aplicación $\lambda_a(x) = a \cdot x$ para todo $x \in R$.
- la aplicación de **multiplicación por la derecha de** a en R y se denota por $\rho_a : R \to R$ como la aplicación $\rho_a(x) = x \cdot a$ para todo $x \in R$.

Proposición 8 (Ejercicio) *Sea R un anillo y sea $a \in R$. Entonces:*

- *a no es divisor de cero por la izquierda si y sólo si $\lambda_a : R \to R$ es una aplicación inyectiva.*
- *a no es divisor de cero por la derecha si y sólo si $\rho_a : R \to R$ es una aplicación inyectiva.*

- *Si a es inversible, $\lambda_a : R \to R$ es biyectiva.*
- *Si a es inversible, $\rho_a : R \to R$ es biyectiva.*
- *Si R es conmutativo y unitario, a es inversible si y sólo si $\lambda_a : R \to R$ es biyectiva.*
- *Si R es conmutativo y unitario, a es inversible si y sólo si $\rho_a : R \to R$ es biyectiva.*
- *Si en R no hay divisores de cero, a es inversible si y sólo si $\lambda_a : R \to R$ es biyectiva.*
- *Si en R no hay divisores de cero, a es inversible si y sólo si $\rho_a : R \to R$ es biyectiva.*

Teorema 9 Todo dominio de integridad finito es cuerpo.

Demo: Sea D un dominio de integridad finito y $0 \neq a \in D$. Veamos que a es un elemento inversible de D. Consideremos la aplicación de multiplicación por la izquierda de a en R,

$$\lambda_a : D \to D \quad \text{definida por} \quad \lambda_a(x) = a \cdot x.$$

Como D verifica la ley de cancelación por la izquierda, λ_a es una aplicación inyectiva: si $\lambda_a(x) = \lambda_a(y)$, entonces $ax = ay$, y por tanto, aplicando la ley de simplificación, $x = y$. Ahora, como D es finito, λ_a es sobreyectiva, luego existe $b \in D$ con $ab = \lambda_a(b) = 1$. Por último, como D es conmutativo $ab = ba = 1$ y a es inversible con inverso b. ■

Nota: Esta demostración te puede ayudar a resolver varios ejercicios del tema.

2. Cuerpo de fracciones de un dominio de integridad

En temas anteriores se ha estudiado $\mathbb{Z}$, el anillo de los enteros. Veamos como se puede construir $\mathbb{Q}$ a partir de $\mathbb{Z}$:

Construcción de los racionales.

$\star$ Definimos una relación de equivalencia en el conjunto de los pares $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, en donde $\mathbb{Z}^*$ denota los enteros menos el cero.

Diremos que

$$(a, b) \sim (a', b') \text{ si y sólo si } ab' = a'b.$$

La clase de equivalencia del elemento (a, b) se denota por $\frac{a}{b}$. Sea $\mathbb{Q}$ el conjunto cociente:

$$\mathbb{Q} := \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0\}$$

$\star$ Definimos la suma y el producto en el conjunto cociente:

$\diamondsuit$ La suma: $\frac{a}{b} + \frac{a'}{b'} := \frac{ab'+ba'}{bb'}$.

$\diamondsuit$ El producto: $\frac{a}{b} \cdot \frac{a'}{b'} := \frac{aa'}{bb'}$.

Nos encontramos con que $(\mathbb{Q}, +, .)$ es el cuerpo de los racionales.

En este tema vamos a demostrar que esta construcción no es exclusiva de $\mathbb{Z}$, sino que dado cualquier dominio de integridad D podemos construir un cuerpo Q, tal que D se "sumerge" en Q de forma similar a como $\mathbb{Z}$ se "sumerge" en $\mathbb{Q}$.

Construcción del cuerpo de fracciones de un dominio de integridad.

Aunque la construcción que aquí damos comienza con un dominio de integridad D, realmente no nos van a hacen falta tantas hipótesis, por lo que tras cada una de las demostraciones de las proposiciones de este tema nombraremos las propiedades que se han usado.

Sea D un dominio de integridad. Consideremos

$$D \times D^* := \{(a,b) \in D \times D \mid b \neq 0\}$$

Proposición 1 Sea D un dominio de integridad. Entonces, en $D \times D^*$ la relación,

$$(a,s) \approx (b,r) \text{ si y sólo si } ar = bs,$$

es de equivalencia.

Demo: Veamos que $\approx$ verifica las propiedades reflexiva, simétrica y transitiva:

$\star$ Reflexiva: sea $(a,s) \in D \times D^*$. Entonces $as = as$, con lo que $(a,s) \approx (a,s)$.

$\star$ Simétrica: Supongamos que $(a,s) \approx (b,r)$. Entonces, $ar = bs$ que directamente da $(b,r) \approx (a,s)$.

$\star$ Transitiva: Supongamos que $(a,s) \approx (b,r)$ y $(b,r) \approx (c,t)$. Entonces:

$$ar = bs \quad \text{y} \quad bt = cr.$$

$\star$ Multiplicamos en la primera igualdad por t y $art = bst$.
$\star$ Sustituimos bt por cr (segunda igualdad) obtenemos $art = bts = crs$.
$\star$ Simplificando r, ya que es no nulo y D verificar las leyes de simplificación, $at = cs$. Es decir, $(a,s) \approx (c,t)$. ■

Observación 2 *Las propiedades reflexivas y simétricas solo necesitan que D sea un anillo. Mientras que la propiedad transitiva necesita que los denominadores no sean divisores de cero y conmuten entre sí.*

Definición 3 *El conjunto cociente anterior, $D \times D^*/\approx$, se denotará por $\mathcal{Q}(D)$. La clase de equivalencia de un elemento $(a,s) \in D \times D^*$ será denotada por $\frac{a}{s}$. Dado un elemento $\frac{a}{s} \in \mathcal{Q}(D)$, diremos que a es el numerador y s el denominador.*

Observación: En toda las demostraciones intentaremos usar letras tipo a, b, c, d para los numeradores y s, r, t para los denominadores (en algunos casos con primas, a', s').

Teorema 4 Sea D un dominio de integridad. Entonces, en $\mathcal{Q}(D)$, las operaciones

$$\diamondsuit \text{ Suma:} \qquad \frac{a}{s} + \frac{b}{r} := \frac{ar+bs}{rs}$$

$$\diamondsuit \text{ Producto:} \quad \frac{a}{s} \cdot \frac{b}{r} := \frac{ab}{rs}$$

dotan a $\mathcal{Q}(D)$ de estructura de cuerpo (llamado el **cuerpo de fracciones** del dominio de integridad D). Es más, la aplicación $i : D \to \mathcal{Q}(D)$ definida por $i(d) = \frac{d}{1}$ es un monomorfismo de anillos unitarios.

Demo: Veamos que la suma anterior define una estructura de grupo abeliano en $\mathcal{Q}(D)$, para ello tendremos que demostrar:

(i). Que está bien definida (hace falta ver que el elemento $(ar+bs, rs) \in D \times D^*$ y que esta suma no depende de los representantes.
(i.1) Es claro que $rs \neq 0$ ya que D es un dominio de integridad y $s \neq 0 \neq r$.
(i.2) Veamos que esta suma no depende de los representantes. Supongamos que $(a,s) \approx (a',s')$ y que $(b,r) \approx (b',r')$. Tenemos entonces que:

$$as' = a's \quad \text{y} \quad br' = b'r \tag{H}$$

y queremos demostrar que $(ar+bs, rs) \approx (a'r'+b's', r's')$:

$$\begin{aligned}(ar+bs)r's' &=^{*^1} arr's' + bsr's' =^{*^2} (as')rr' + (br')ss' = \\ &=^{*^3} (a's)rr' + (b'r)ss' =^{*^2} a'r'sr + b's'sr =^{*^1} (a'r'+b's')rs\end{aligned}$$

$*^1$ aplicando la propiedad asociativa y la distributiva.
$*^2$ aplicando la propiedad asociativa y la conmutativa.
$*^3$ aplicando las identidades de (H).
$*^4$ aplicando la propiedad asociativa, la conmutativa y la distributiva.
Luego la suma está bien definida en $\mathcal{Q}(D)$.

(ii). Veamos ahora que $(\mathcal{Q}(D), +)$ tiene estructura de grupo abeliano. Antes veamos algunas propiedades útiles:

(P_1). Dado un elemento no nulo $r \in D$, para todo $\frac{a}{s} \in \mathcal{Q}(D)$, $\frac{a}{s} = \frac{ra}{rs}$.

(P_2). Dos elementos $\frac{a}{s}$, $\frac{b}{r}$ de $\mathcal{Q}(D)$ tienen representantes con el mismo denominador:

$$\frac{a}{s} = \frac{ar}{rs} \text{ y } \frac{b}{r} = \frac{bs}{rs}.$$

Naturalmente, con este proceso se consigue encontrar denominador común a un conjunto finito de elementos de $\mathcal{Q}(D)$.

(P_3). La suma de dos elementos $\frac{a}{s}$ y $\frac{b}{s}$ con el mismo denominador consiste en sumar numeradores:

$$\frac{a}{s} + \frac{b}{s} = \frac{as+bs}{s^2} = \frac{a+b}{s}$$

con estas tres propiedades, ya podemos demostrar fácilmente que $(\mathcal{Q}(D), +)$ tiene estructura de grupo abeliano. Por P_2 voy a tomar, cuando me sea de interés, "fracciones" con el mismo denominador.

Fin de clase 24; 29-11-2011, grupos A y B.

(ii.1) Asociativa: sean $\frac{a}{s}, \frac{b}{s}, \frac{c}{s} \in \mathcal{Q}(D)$. Entonces:

$$\left(\frac{a}{s} + \frac{b}{s}\right) + \frac{c}{s} = \frac{a+b}{s} + \frac{c}{s} = \frac{a+b+c}{s} = \frac{a}{s} + \frac{b+c}{s} = \frac{a}{s} + \left(\frac{b}{s} + \frac{c}{s}\right)$$

(ii.2) Conmutativa: sean $\frac{a}{s}, \frac{b}{s} \in \mathcal{Q}(D)$. Entonces:

$$\frac{a}{s} + \frac{b}{s} = \frac{a+b}{s} = \frac{b+a}{s} = \frac{b}{s} + \frac{a}{s}$$

(ii.3) El neutro de la suma es cualquier elemento de la forma $\frac{0}{s}$ con $s \in D^*$.
(ii.4) Opuesto: dado $\frac{a}{s} \in \mathcal{Q}(D)$, $\frac{-a}{s}$ es su opuesto, ya que $\frac{a}{s} + \frac{-a}{s} = \frac{0}{s} = 0$.

(iii). Veamos ahora que el producto está bien definido: (hace falta ver que el elemento $(ab, rs) \in D \times D^*$ y que este producto no depende de los representantes.
(iii.1) Es claro que $rs' \neq 0$ ya que D es un dominio de integridad y $s \neq 0 \neq r$.
(iii.2) Veamos que el producto no depende de los representantes. Supongamos que $(a, s) \approx (a', s')$ y que $(b, r) \approx (b', r')$. Tenemos entonces que:

$$as' = a's \quad \text{y} \quad br' = b'r \tag{H'}$$

Tenemos que demostrar que $(ab, rs) \approx (a'b', r's')$:

$$abr's' = (as')(br') = (a's)(b'r) = a'b'rs.$$

(iii.3) Asociativa: sean $\frac{a}{s}, \frac{b}{r}, \frac{c}{t} \in \mathcal{Q}(D)$. Entonces:

$$\left(\frac{a}{s} \cdot \frac{b}{r}\right) \cdot \frac{c}{t} = \frac{ab}{rs} \cdot \frac{c}{t} = \frac{abc}{rst} = \frac{a}{s} \cdot \frac{bc}{rt} = \frac{a}{s} \cdot \left(\frac{b}{r} \cdot \frac{c}{t}\right)$$

(iv). Distributiva: demostramos sólo la distributiva por un lado, ya que vamos a demostrar que el producto es conmutativo. Sean $\frac{a}{s}, \frac{b}{s}, \frac{c}{t} \in \mathcal{Q}(D)$. Entonces:

$$\left(\frac{a}{s} + \frac{b}{s}\right) \cdot \frac{c}{t} = \frac{a+b}{s} \cdot \frac{c}{t} = \frac{(a+b)c}{st} = \frac{ac+bc}{st} = \frac{ac}{ct} + \frac{bc}{st} = \frac{a}{s} \cdot \frac{c}{t} + \frac{b}{s} \cdot \frac{c}{t}$$

(v). $\mathcal{Q}(D)$ es un cuerpo (anillo conmutativo, unitario en donde todo elemento no nulo tiene inverso):
(v.1) Conmutativa: sean $\frac{a}{s}, \frac{b}{r} \in \mathcal{Q}(D)$. Entonces:

$$\frac{a}{s} \cdot \frac{b}{r} = \frac{ab}{rs} = \frac{ba}{rs} = \frac{b}{r} \cdot \frac{a}{s}$$

(v.2) La unidad de $\mathcal{Q}(D)$: el elemento $\frac{1}{1} = \frac{s}{s}$ para todo $s \in D^*$, es el elemento neutro de la suma.
(v.3) Sea $\frac{a}{s}$ un elemento no nulo de $\mathcal{Q}(D)$. Como es no nulo, ver (ii.3), $a \neq 0$ y por tanto, $\frac{s}{a}$ tiene sentido, y es el inverso de $\frac{a}{s}$:

$$\frac{s}{a}\frac{a}{s} = \frac{sa}{as} = \frac{1}{1}$$

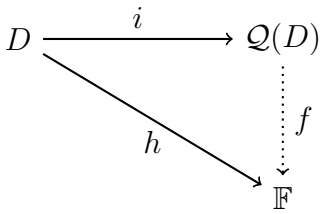
(vi). Veamos que la aplicación $i : D \to \mathcal{Q}(D)$, definida por $i(d) := \frac{d}{1}$, es un monomorfismo de anillos.

$$i(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = i(a) + i(b)$$
$$i(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = i(a)i(b)$$

Por último si $i(b) = 0$, entonces $\frac{b}{1} = \frac{0}{1}$ por lo que $b \cdot 1 = 0 \cdot 1 = 0$ y $b = 0$, es decir, i es una aplicación inyectiva. ■

Corolario 5 Un anillo D es un dominio de integridad si y sólo si es subanillo (unitario) de un cuerpo.

Teorema 6 (Ejercicio) Sea D un dominio de integridad, $\mathbb{F}$ un cuerpo y $h : D \to \mathbb{F}$ un monomorfismo de anillos. Entonces existe un único monomorfismo de anillos $f : \mathcal{Q}(D) \to \mathbb{F}$ que hace conmutativo el diagrama.



Demo: En principio nos dicen que existe un único homomorfismo f de $\mathcal{Q}(D)$ en $\mathbb{F}$ que hace conmutativo el diagrama. Veamos en primer lugar que podemos saber de f (supongamos que existe un homomorfismo f y veamos como tiene que definirse):

Dado $d \in D$, como el diagrama es conmutativo,

$$h(d) = f \circ i(d) = f(d/1).$$

Por otro lado, como i y h son aplicaciones inyectivas, si d' es un elemento no nulo de D, $i(d') = d'/1$ es un elemento no nulo de $\mathcal{Q}(D)$, $h(d')$ es un elemento no nulo de $\mathbb{F}$ y $f(d'/1)$ es un elemento no nulo de $\mathbb{F}$. Por tanto estos elementos son inversibles por lo que

$$f(1/d') = f(d'/1)^{-1} = h(d')^{-1}$$

Por tanto, tenemos una única forma de definir f: Dado $a/r \in \mathcal{Q}(D)$,

$$f(a/r) = f(a/1 \cdot 1/r) = f(a/1) \cdot f(1/r) = h(a)h(r)^{-1}$$

Veamos que esta única forma de definir f es un monomorfismo de anillos que hace conmutativo el diagrama:

i). Veamos que f está bien definida: Si $a/r = a'/r'$, entonces $ar' = a'r$, por lo que $h(a)h(r') = h(ar') = h(a'r) = h(a')h(r)$. Como $h(r)$ y $h(r')$ son no nulos, podemos multiplicar por sus inversos, con lo que $h(a) = h(a)h(r')h(r')^{-1} = h(a')h(r)h(r')^{-1} = h(a')h(r')^{-1}h(r)$ y multiplicando pro el inverso de $h(r)$, $h(a)h(r)^{-1} = h(a')h(r')^{-1}$, es decir, $f(a/r) = f(a'/r')$.

ii). Veamos que es un homomorfismo de anillos:

$$\begin{aligned}
\star\ f(a/r + b/r) &= f((a+b)/r) = h(a+b)h(r)^{-1} = (h(a) + h(b))h(r)^{-1} \\
&= h(a)h(r)^{-1} + h(b)h(r)^{-1} = f(a/r) + f(b/r) \\
\star\ f(a/r \cdot b/s) &= f(ab/rs) = h(ab)h(rs)^{-1} = h(a)h(b)(h(r)h(s))^{-1} = h(a)h(b)h(s)^{-1}h(r)^{-1} \\
&= h(a)h(r)^{-1}h(b)h(s)^{-1} = f(a/r)f(b/s)
\end{aligned}$$

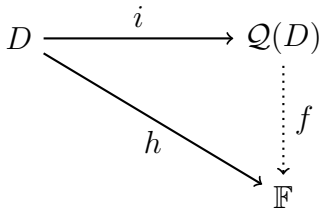
iii). Veamos que f es un monomorfismo de anillos: sea $a/r \in \mathrm{Ker}(f)$. Entonces $0 = f(a/r) = h(a)h(r)^{-1}$, multiplicando, en ambos miembros, por $h(r)$, $h(a) = 0$ y como h es un monomorfismo de anillos, $a = 0$, por lo que $a/r = 0/r$, es decir, $\mathrm{Ker}(f) = \{0\}$ y por tanto f es inyectiva. ■

Poner parte del complemento como ejercicios?

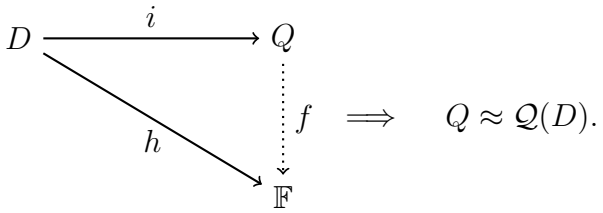
3. Complemento de la Teoría

La segunda parte importante del cuerpo de fracciones $\mathcal{Q}(D)$ de un dominio de integridad D es que es el cuerpo "más pequeño" que contiene a D. Naturalmente la noción de "ser más pequeño que" significa (este teorema es complemento del anterior):

Teorema 1 Sea D un dominio de integridad, $\mathbb{F}$ un cuerpo y $h : D \to \mathbb{F}$ un monomorfismo de anillos. Entonces existe un único monomorfismo de anillos $f : \mathcal{Q}(D) \to \mathbb{F}$ que hace conmutativo el diagrama.



Es más, si Q es un cuerpo tal que existe un monomorfismo de anillos $i : D \to Q$ y tal que para cada cuerpo $\mathbb{F}$ y cada monomorfismo de anillos $h : D \to \mathbb{F}$, existe un único monomorfismo de anillos $f : Q \to \mathbb{F}$ que hace conmutativo el diagrama. Se tiene que Q es isomorfo al cuerpo de fracciones de D.



En todo este tema hemos partido de D, un dominio de integridad, pero ¿nos hacia falta tanto?

Corolario 2 Un anillo R es conmutativo y sin divisores de cero si y sólo si es subanillo de un cuerpo.

Si nos fijamos bien en la demostraciones que hemos hecho, ¿donde se usa que D sea unitario?

En la proposición 1 (Pag. 89) no se usa el carácter unitario: la relación $(a, b) \approx (a', b')$ si y sólo si $ab' = a'b$ es de equivalencia, sea D unitario o no.

El Teorema 4 (Pag. 89) demuestra que el conjunto cociente, $\mathcal{Q}(D)$ con las operaciones definidas tiene estructura de anillo (aquí no hace falta la unidad. Para demostrar que $\mathcal{Q}(D)$ es un cuerpo (luego unitario), parece ser que sí. No obstante, dado $0 \neq a \in D$, $\frac{a}{a}$ es la unidad de $\mathcal{Q}(D)$ y el inverso de un elemento no nulo $\frac{b}{a}$ sigue siendo $\frac{a}{b}$. Por lo que la unidad de D, en realidad, no ha hecho falta.

Si nos damos cuenta, los últimos teoremas tampoco hacen uso de que D tiene un elemento unitario.

Definición 3 Sea R un anillo. Se define $Z(R)$, el centro de R, como:

$$Z(R) = \{z \in R \mid za = az \quad \forall\, a \in R\}$$

Definición 4 Sea R un anillo. Se dice que un subconjunto $S \subset R$ es un conjunto de denominadores para R si.

- $S \subset Z(R)$,
- S no contiene divisores de cero y
- $S \cdot S \subset S$ (S es un subconjunto multiplicativamente cerrado de R).

Corolario 5 Sea R un anillo y sea $S \subset R$ es un conjunto de denominadores para R. Entonces existe un anillo Q que contiene a R como subanillo y tal que todo elemento de S es inversible en Q.

Se puede dar una construcción idéntica a la construcción del cuerpo de fracciones:

⋆ Se considera el conjunto $R \times S$ y la relación $(a, s) \approx (b, r)$ si y sólo si $ar = bs$. Se comprueba que es un relación de equivalencia. La clase de equivalencia de un elemento (a, s) se denota por $\frac{a}{s}$ y el conjunto cociente por $S^{-1}R$.

⋆ Se define una suma y un producto en $S^{-1}R$ como:

- La suma: $\frac{a}{s} + \frac{b}{r} := \frac{ar+bs}{rs}$.
- El producto: $\frac{a}{s} \cdot \frac{b}{r} := \frac{ab}{rs}$.

Siguiendo la demostración del Teorema 4 (Pag. 89) se demuestra que $(S^{-1}R, +, \cdot)$ tiene estructura de anillo que tiene la propiedad que todo elemento de S es inversible en $S^{-1}R$.

Nota: Observar que el Teorema 4 (Pag. 89) es consecuencia de este último resultado: si D es un dominio de integridad puedo considerar como conjunto de denominadores D^* (comprobar que verifica las tres propiedades) y el anillo $S^{-1}D$ es precisamente $\mathcal{Q}(D)$, el cuerpo de fracciones del dominio de integridad D.

4. Ejercicios del Tema

1 Sea $D = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

(i) Demuestra que D es un dominio de integridad.

(ii) Calcula el cuerpo de fracciones de D, denotado por $\mathcal{Q}(D)$, y da el único monomorfismo $f : \mathcal{Q}(D) \to \mathbb{R}$ que es la inclusión cuando restringimos a D.

(iii) Por si no te has dado cuenta, demuestra que $\mathcal{Q}(D) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Calcula el inverso de $2 + 3\sqrt{2}$ y dalo en la forma $a + b\sqrt{2}$ con $a, b \in \mathbb{Q}$.

2 Sea D un dominio de integridad y D' un subanillo unitario de D. Demuestra que D' es también un dominio de integridad. ¿El cuerpo de fracciones de D y D' coinciden?

3 Calcula el menor subanillo unitario de $\mathbb{R}$ que contiene a $\sqrt[3]{5}$. [∗]

4 Sea R un anillo sin divisores de cero y sea $e \in R$ un elemento no nulo tal que $e^2 = e$. Demuestra que R es un anillo unitario. [∗]

5 Sea D y D' dos dominios de integridad y $f : D \to D'$ un monomorfismo de anillos. ¿Puedes encontrar un homomorfismo de anillos $\bar{f} : \mathcal{Q}(D) \to \mathcal{Q}(D')$ tal que $\bar{f}(\frac{b}{1}) = \frac{f(b)}{1}$? ¿Y si f no es un monomorfismo?

6 *Sea R un anillo y sea $a \in R$. Entonces:*

- *a no es divisor de cero por la izquierda si y sólo si $\lambda_a : R \to R$ es una aplicación inyectiva.*
- *a no es divisor de cero por la derecha si y sólo si $\rho_a : R \to R$ es una aplicación inyectiva.*
- *Si a es inversible, $\lambda_a : R \to R$ es biyectiva.*
- *Si a es inversible, $\rho_a : R \to R$ es biyectiva.*
- *Si R es conmutativo y unitario, a es inversible si y sólo si $\lambda_a : R \to R$ es biyectiva.*
- *Si R es conmutativo y unitario, a es inversible si y sólo si $\rho_a : R \to R$ es biyectiva.*
- *Si en R no hay divisores de cero, a es inversible si y sólo si $\lambda_a : R \to R$ es biyectiva.*
- *Si en R no hay divisores de cero, a es inversible si y sólo si $\rho_a : R \to R$ es biyectiva.*

7 Sea R un anillo unitario y finito y sea $a \in R$ que no es divisor de cero por la izquierda. Entonces a es inversible. [∗]

8 Sea R un anillo unitario y finito y sea $a \in R$ que no es divisor de cero por la izquierda. Entonces a no es divisor de cero por la derecha. [∗]

9 Sea R un anillo finito y sea $a \in R$ que no es divisor de cero (ni por la izquierda ni por la derecha). Entonces R es unitario. [∗∗]

10 Si D es dominio de integridad, $D[X]$ es dominio de integridad. ¿Será el cuerpo de fracciones de $D[X]$ el anillo de polinomios sobre el cuerpo de fracciones de D?

11 Encuentra dos dominios de integridad, $D \subset D'$ tales que $\mathcal{Q}(D) = \mathcal{Q}(D')$ (aquí el igual puede significar isomorfos).

12 Encuentra dos dominios de integridad, $D \subset D'$ tales que $\mathcal{Q}(D) \neq \mathcal{Q}(D')$ (aquí el igual puede significar no isomorfos).

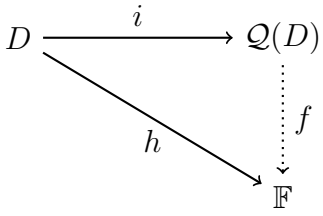
13 Demuestra que $\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{R}$. [$*$]

14 Demuestra que $\mathbb{Z} + \mathbb{Z}i$ es un subanillo de $\mathbb{C}$ que es dominio de integridad. Demuestra que el cuerpo de fracciones de $\mathbb{Z} + \mathbb{Z}i$ es $\mathbb{Q} + \mathbb{Q}i$. [$*$]

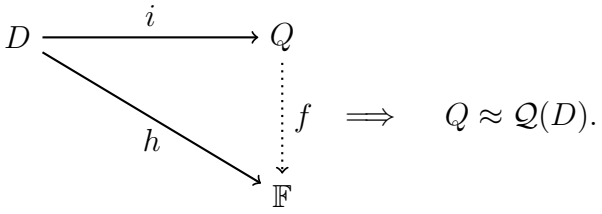
15 Sea D un dominio de integridad de característica p (p un número primo). Demuestra que la característica de $\mathcal{Q}(D)$ es también p.

16 Sea D un dominio de integridad y sean n elementos $\frac{a_i}{s_i} \in \mathcal{Q}(D)$, $i = 1, \ldots, n$. Demuestra que puedes encontrar representantes de estos elementos con el mismo denominador. ¿Podrías conseguir que este denominador común fuera el mínimo común múltiplo de $\{s_1, s_2, \ldots, s_n\}$?

17 Sea D un dominio de integridad, $\mathbb{F}$ un cuerpo y $h : D \to \mathbb{F}$ un monomorfismo de anillos. Demuestra que existe un único monomorfismo de anillos $f : \mathcal{Q}(D) \to \mathbb{F}$ que hace conmutativo el diagrama. [$*$]



18 Sea D un dominio de integridad y sea Q un cuerpo tal que existe un monomorfismo de anillos $i : D \to Q$ tal que para cada cuerpo $\mathbb{F}$ y cada monomorfismo de anillos $h : D \to \mathbb{F}$, existe un único monomorfismo de anillos $f : Q \to \mathbb{F}$ que hace conmutativo el diagrama. Se tiene que Q es isomorfo a $\mathcal{Q}(D)$, cuerpo de fracciones de D. [$*$]



Algunos ejercicios de temas anteriores

19 Sea R un anillo y sea $S \leq R$. ¿Que puedes decir de la característica de R y S? [$**$]

20 Sea $n \in \mathbb{N}$. Entonces un elemento $\overline{a} \in \mathbb{Z}_n$ o es inversible o es divisor de cero. [$*$]

21 Encuentra un anillo R y un elemento $x \in R$ tal que x no sea ni inversible ni divisor de cero.

22 Sea R un anillo. Demuestra que un elemento inversible no puede ser divisor de cero. En particular, demuestra en un anillo de división (y por tanto en un cuerpo) no hay divisores de cero.

23 Demuestra que un anillo unitario y finito sin divisores de cero por la derecha (o por la izquierda) es un anillo de división. [$*$]

Capítulo 5

Anillo cociente

Objetivos del capítulo

- En este capítulo vamos a estudiar cuando una relación de equivalencia-partición en un anillo dota al conjunto cociente de estructura de anillo, con lo que mezclaremos los conceptos de partición de equivalencia-relación con la estructura de anillo. Caracterizaremos las relaciones de equivalencia que dan lugar a conjuntos cocientes con estructura de anillo, lo que nos llevará a la definición de ideal.
- Estudiaremos los ideales de un anillo y sus propiedades.
- Introduciremos la noción de anillo cociente y estudiaremos sus propiedades.

---

1. Introducción

Dado un anillo R y una relación de equivalencia, $\approx$, en R vamos a estudiar cuando podemos definir una estructura de anillo en el conjunto cociente $R/\approx$, en donde la suma y el producto se hereden de R. Es decir, en donde la suma y el producto queden definidos por:

$$\overline{x} + \overline{y} := \overline{x+y}$$
$$\overline{xy} := \overline{xy}$$

Nota 1: No siempre es posible.

Nota 2: Recordamos que lo elementos del conjunto cociente $R/\approx$ son subconjunto de R. Así, dado un $x \in R$, la clase del x, que se denota por $\overline{x}$, representa al subconjunto $\overline{x} = \{y \in R | x \approx y\}$. Es más, por el Teorema 7 (Pag. 17) tenemos que

$$x \approx y \iff x \in \overline{y} \iff y \in \overline{x} \iff \overline{x} = \overline{y}.$$

Nos encontramos con que no siempre la suma o el producto anterior están bien definidos. Es decir, podemos tener una relación de equivalencia en R tal que $\overline{x_1} = \overline{x_2}$, $\overline{y_1} = \overline{y_2}$ pero

- $\overline{x_1 + y_1} \neq \overline{x_2 + y_2}$, lo que implicaría que la operación suma en el conjunto cociente $R/\approx$ está mal definida o
- $\overline{x_1 \cdot y_1} \neq \overline{x_2 \cdot y_2}$, lo que implicaría que la operación producto en el conjunto cociente $R/\approx$ está mal definida.

Realmente ya nos hemos encontrado con este problema anteriormente:

Ejemplos A *Sea $\mathbb{Z}$ el anillo de los enteros. Consideremos en $\mathbb{Z}$ la relación de congruencias modulo n. Tenemos que el conjunto cociente en está relación es*

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

En este conjunto definimos una suma y un producto demostrando que ambos estaban bien definidos (tanto la suma como el producto no dependía de los representantes), ver el teorema 3 (Pag. 40).

Ejemplos B *Sea $\mathbb{Z}$ el anillo de los enteros. Consideremos en $\mathbb{Z}$ la relación de equivalencia*

$$x \sim y \text{ si } y \text{ sólo si } x = y = 0 \text{ o } x \cdot y > 0$$

Tenemos que el conjunto cociente tiene tres clases de equivalencia:

$$\overline{0} = \{0\}, \quad \overline{1} = \{x \in \mathbb{Z} | x > 0\} \quad y \quad \overline{-1} = \{x \in \mathbb{Z} | x < 0\}.$$

No obstante en este conjunto cociente la suma no está bien definida: $\overline{1} = \overline{3}$ y $\overline{-1} = \overline{-4}$, pero

$$\overline{0} = \overline{1} + \overline{-1} = \overline{3} + \overline{-4} = \overline{-1}$$

En cambio, el producto si que está bien definido!!!

2. Ideales de un anillo. El anillo cociente.

Teorema 1 Sea R un anillo y $\approx$ una relación de equivalencia en R tal que en el conjunto cociente, $R/\approx$, las siguientes operaciones están bien definidas.

$$\overline{x} + \overline{y} := \overline{x+y}$$
$$\overline{xy} := \overline{xy}$$

Entonces:

(i) $(R/\approx, +, \cdot)$ tiene estructura de anillo. (Ejercicio)

(ii) $\overline{0}$ es un subanillo de R tal que para todo $a \in R$ e $x \in \overline{0}$, $a \cdot x \in \overline{0}$ y $x \cdot a \in \overline{0}$.

(iii) Dos elementos $a, b \in R$ están relacionados, $a \approx b$, si y sólo si $a - b \in \overline{0}$.

Demo: (i) Ejercicio.
(ii). Veamos que $\overline{0} = \{x \in R | 0 \approx x\}$ es un subanillo de R:
• La suma es una operación interna en $\overline{0}$: dados $x, y \in \overline{0}$, por hipótesis tenemos que $\overline{x} = \overline{0} = \overline{y}$, por tanto, como la suma está bien definida,

$$\overline{x+y} = \overline{x} + \overline{y} = \overline{0} + \overline{0} = \overline{0+0} = \overline{0}$$

con lo que $x + y \in \overline{0}$.
• El producto es una operación interna en $\overline{0}$: dados $x, y \in \overline{0}$, por hipótesis tenemos que $\overline{x} = \overline{0} = \overline{y}$, por tanto, como el producto está bien definido,

$$\overline{x \cdot y} = \overline{x} \cdot \overline{y} = \overline{0} \cdot \overline{0} = \overline{0 \cdot 0} = \overline{0}$$

con lo que $x \cdot y \in \overline{0}$.

- Como $0 \approx 0$, tenemos que $0 \in \overline{0}$.
- Sea $x \in \overline{0}$ y sea $-x \in R$, el opuesto de x en R. Tenemos,

$$\overline{0} = \overline{x + (-x)} = \overline{x} + \overline{-x} = \overline{0} + \overline{-x} = \overline{-x}.$$

Por tanto $-x \in \overline{0}$.

Por último, dado $x \in \overline{0}$ y $a \in R$,

$$\overline{a \cdot x} = \overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{0} = \overline{a \cdot 0} = \overline{0}$$
$$\overline{x \cdot a} = \overline{x} \cdot \overline{a} = \overline{0} \cdot \overline{a} = \overline{0 \cdot a} = \overline{0}$$

Lo que demuestra que $a \cdot x$ y $x \cdot a$ pertenecen a $\overline{0}$.

(iii). Sean $a, b \in R$.

- Supongamos que $a \approx b$. Entonces $\overline{a} = \overline{b}$ y por tanto

$$\overline{0} = \overline{b + (-b)} = \overline{b} + \overline{-b} = \overline{a} + \overline{-b} = \overline{a - b}$$

Por lo que $a - b \in \overline{0}$.

- Supongamos ahora que $a - b \in \overline{0}$. Tenemos entonces que

$$\overline{b} = \overline{b} + \overline{0} = \overline{b} + \overline{a - b} = \overline{b + a - b} = \overline{a},$$

por lo que $a \approx b$. ■

Fin de clase 25; 01-12-2011, grupos A y B.

Definición 2 Sea R un anillo. Se dice que $I \subset R$ es un **ideal** de R si I es un subanillo de R tal que para todo $a \in R$, $y \in I$, $ay, ya \in I$.

Ejemplos A *Sea R un anillo, entonces R y $\{0\}$ son siempre ideales de R (llamados triviales). Sea $\mathbb{Z}$ el anillo de los enteros. Entonces para cada $n \in \mathbb{N}$ el conjunto $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$.*

Nota: Para demostrar que un subconjunto es un ideal habría que demostrar 5 propiedades (las cuatro de subanillo y la propia de ideal). No obstante, el siguiente lema reduce el proceso:

Lema 3 Sea R un anillo y sea $I \subset R$. Entonces I es un ideal de R si y sólo si $I \neq \emptyset$ y

(i) La suma es una operación interna en I.
(ii) Para todo $a \in I$, $-a \in I$.
(iii) Para todo $a \in R$, $y \in I$, $ay, ya \in I$.

Demo: Es claro que si I es un ideal verifica estas tres condiciones. Supongamos que un subconjunto I de un anillo R verifica estas tres condiciones. (iii) implica que el producto es una operación cerrada en I. Es más, dado $y \in I$ y $0 \in R$, $0 = 0 \cdot y \in I$, lo que demuestra que I es un subanillo, y por tanto un ideal de R. ■

Nota: En el siguiente Teorema vamos a ver una especie de recíproco del Teorema 1 (Pag. 98): en este último vemos que si las operaciones están bien definidas, $\overline{0}$ es un ideal de R y la relación de equivalencia está asociada a este ideal. En el siguiente teorema demostramos que todo ideal define una relación de equivalencia en R en donde la suma y el producto procedentes de R están bien definidos en conjunto cociente:

Teorema 4 Sea R un anillo e I un ideal de R. Entonces:

(i) La relación $x \sim y$ si y solo si $x - y \in I$ es una relación de equivalencia en R.

(ii) $(R/\sim, +, \cdot)$ en donde

$$\bar{x} + \bar{y} := \overline{x+y}$$
$$\bar{x} \cdot \bar{y} := \overline{x \cdot y}$$

tiene estructura de anillo.

El anillo anterior se denota por R/I y se llama el **anillo cociente de R sobre I**.

Demo: (i). Reflexiva: $x - x = 0 \in I$, por lo que $x \sim x$. Transitiva: supongamos que $x \sim y$ y que $y \sim z$. Tenemos entonces que $x - y \in I$ y que $y - z \in I$. Por tanto $x - z = x - y + y - z \in I$ lo que implica que $x \sim z$. Simétrica: Si $x \sim y$, $x - y \in I$. Por tanto $y - x = -(x - y) \in I$, lo que implica que $y \sim x$.

(ii). Empecemos demostrando que suma y producto están bien definidas: Sean $x, x', y, y' \in R$ tales que $x \sim x'$ e $y \sim y'$. tenemos entonces que $x - x' \in I$ e $y - y' \in I$. Por tanto:

$$(x + y) - (x' + y') = x - x' + y - y' \in I$$

Lo que demuestra que $\overline{x} + \overline{y} = \overline{x'} + \overline{y'}$.

$$x \cdot y - x' \cdot y' = x \cdot y - x \cdot y' + x \cdot y' - x' \cdot y' = x \cdot (y - y') + (x - x') \cdot y' \in I$$

Lo que demuestra que $\overline{x} \cdot \overline{y} = \overline{x'} \cdot \overline{y'}$.

Veamos ahora que estas operaciones dotan de estructura de anillo al conjunto cociente:

• $(R/\sim, +)$ es un grupo abeliano: para todo $\overline{a}, \overline{b}, \overline{c} \in R/\sim$.

⋆ Propiedad asociativa:

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{a+b+c} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c})$$

⋆ Elemento neutro: $\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$.

⋆ Elemento opuesto: dado $\overline{a} \in R/\sim$ su opuesto es $\overline{-a} \in R/\sim$.

⋆ Propiedad conmutativa: $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$.

• $(R, \cdot)$ verifica la propiedad asociativa: para todo $\overline{a}, \overline{b}, \overline{c} \in R/\sim$.

$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a \cdot b} \cdot \overline{c} = \overline{a \cdot b \cdot c} = \overline{a} \cdot \overline{b \cdot c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$$

• Se verifican las propiedades distributivas: para todo $\overline{a}, \overline{b}, \overline{c} \in R/\sim$,

$$(\overline{a} + \overline{b}) \cdot \overline{c} = \overline{a+b} \cdot \overline{c} = \overline{(a+b) \cdot c} = \overline{a \cdot c + b \cdot c} = \overline{a \cdot c} + \overline{b \cdot c} = \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c}$$
$$\overline{c} \cdot (\overline{a} + \overline{b}) = \overline{c} \cdot \overline{a+b} = \overline{c \cdot (a+b)} = \overline{c \cdot a + c \cdot b} = \overline{c \cdot a} + \overline{c \cdot b} = \overline{c} \cdot \overline{a} + \overline{c} \cdot \overline{b}$$

Lo que demuestra el teorema. ■

Nota: Trabajar en un anillo cociente es fácil: sea R un anillo y sea I un ideal de R. Consideremos el anillo cociente R/I. Entonces:

- La suma: $\overline{x} + \overline{y} = \overline{x+y}$
- El producto: $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$
- Dos elementos $\overline{x}, \overline{y} \in R/I$ son iguales $(\overline{x} = \overline{y})$ si y sólo si $x - y \in I$.

- $\overline{x}$ es el elemento neutro ($\overline{x} = \overline{0}$) si y sólo si $x \in I$.

Si miramos la construcción del anillo de congruencias módulo n, ver el Teorema 3 (Pag. 40), tenemos que es la construcción del anillo cociente $\mathbb{Z}$ sobre $n\mathbb{Z}$, es decir:

Ejemplos B *Sea $\mathbb{Z}$ el anillo de los enteros y $n \in \mathbb{N}$. Entonces $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.*

Asociado a cada estructura hay asociado un homomorfismo:

Definición 5 Sea R un anillo y I un ideal de R. Entonces la aplicación $\pi : R \to R/I$ definida por $\pi(r) = \overline{r}$ es un epimorfismo de anillos (llamado el epimorfismo de **proyección** de R en R/I).

Nota: Recordamos que dado un homomorfismo de anillos $f : R \to R'$ el núcleo o Ker de f consistía en el conjunto $\operatorname{Ker} f := \{x \in R \mid f(x) = 0\}$. Observar dado un anillo R y un ideal I de R, el núcleo de la proyección canónica $\pi : R \to R/I$ es precisamente I.

Teorema 6 (Propiedad fundamental del cociente) Sean R y R' dos anillos y sea $f : R \to R'$ un homomorfismo de anillos. Sea I un ideal de R tal que $I \subset \operatorname{Ker}(f)$. Entonces la aplicación $\bar{f} : R/I \to R'$ definida por $\bar{f}(\bar{x}) := f(x)$ es un homomorfismo de anillos.

Demo: Ejercicio. ■

Teorema 7 (Primer teorema de Isomorfía) Sean R y R' dos anillos y $f : R \to R'$ un homomorfismo de anillos. Entonces:

(i) $\operatorname{Ker}(f) \triangleleft R$.

(ii) $R/\operatorname{Ker}(f) \approx Im(f)$. Es más, la aplicación $\bar{f} : R/\operatorname{Ker}(f) \to Im(f)$ definida por $\bar{f}([x]) := f(x)$ es un isomorfismo de anillos.

Demo: (i). Demostremos las propiedades de ideal: Ya sabemos que $\operatorname{Ker}(f)$ es un subanillo de R, ver el corolario 6(i) (Pag. 62). Por otro lado, dados $z \in \operatorname{Ker}(f)$ y $a \in R$,

$$f(a \cdot z) = f(a) \cdot f(z) = f(a) \cdot 0 = 0$$
$$f(z \cdot a) = f(z) \cdot f(a) = 0 \cdot f(a) = 0$$

Lo que demuestra que $z \cdot a$ y $a \cdot z \in \operatorname{Ker}(f)$.

(ii). Veamos que la aplicación $\bar{f} : R/\operatorname{Ker}(f) \to Im(f)$ definida por $\bar{f}(\overline{x}) := f(x)$ es un isomorfismo de anillos, lo que nos demostrara que $R/\operatorname{Ker}(f)$ y $\operatorname{Im}(f)$ son anillos isomorfos:

• Veamos que $\bar{f}$ está bien definida: Sean $x, y \in R$ tales que $x \approx y$, es decir, $\overline{x} = \overline{y}$. Tenemos entonces que $x - y \in \operatorname{Ker}(f)$ por lo que

$$0 = f(x - y) = f(x) - f(y).$$

Lo que implica que $\bar{f}(\overline{x}) = f(x) = f(y) = \bar{f}(\overline{y})$ o lo que es lo mismo, que $\bar{f}$ está bien definida.

• Veamos que $\bar{f}$ es un homomorfismo de anillos:

$$\bar{f}(\overline{x}+\overline{y}) = \bar{f}(\overline{x+y}) = f(x+y) = f(x)+f(y) = \bar{f}(\overline{x})+\bar{f}(\overline{y})$$
$$\bar{f}(\overline{x}\cdot\overline{y}) = \bar{f}(\overline{x\cdot y}) = f(x+y) = f(x)\cdot f(y) = \bar{f}(\overline{x})\cdot\bar{f}(\overline{y})$$

• Veamos que $\bar{f}$ es biyectiva: Dado $z \in \mathrm{Im}(f)$ tenemos que existe $x \in R$ tal que $f(x) = z$. Por lo que $\bar{f}(\overline{x}) = f(x) = z$, lo que demuestra que $\bar{f}$ es sobreyectiva. Supongamos ahora $\overline{x}$, $\overline{y}$ dos elementos de $R/\operatorname{Ker}(f)$ tales que $\bar{f}(\overline{x}) = \bar{f}(\overline{y})$. Por definición de $\bar{f}$ tenemos que $f(x) = f(y)$ y por tanto $f(x-y) = 0$ lo que implica que $x-y \in \operatorname{Ker}(f)$, o lo que es lo mismo, que $\overline{x} = \overline{y}$, lo que demuestra que $\bar{f}$ es inyectiva. ■

3. El retículo de los ideales de un anillo

En esta sección vamos a estudiar los ideales (ideales por la izquierda, ideales por la derecha) de un anillo R. Como resultados importantes demostraremos que el conjunto de los ideales de un anillo R con la relación de orden "contenido" es un retículo (conjunto ordenado en el que cualquier par de elementos posee supremo).

Definición 1 Sea R un anillo. Se dice que I es un **ideal por la izquierda** de R y se representa por $I \lhd_l R$ si I es un subanillo de R tal que para todo $a \in R$, $y \in I$, $ay \in I$. Se dice que I es un **ideal por la derecha** de R y se representa por $I \lhd_r R$ si I es un subanillo de R tal que para todo $a \in R$, $y \in I$, $ya \in I$.

Nota: Para demostrar que un subconjunto es un ideal por la izquierda (por la derecha) habría que demostrar 5 propiedades [las cuatro de subanillo y la propia de ideal por la izquierda (por la derecha)]. No obstante, el siguiente lema reduce el proceso:

Lema 2 Sea R un anillo y sea $I \subset R$. Entonces I es un ideal por la izquierda (resp. por la derecha) de R si y sólo si $I \neq \emptyset$ y

(i) La suma es una operación interna en I.
(ii) Para todo $a \in I$, $-a \in I$.
(iii) Para todo $a \in R$, $y \in I$, $ay \in I$ (resp. $ya \in I$).

Demo: Es claro que si I es un ideal por la izquierda o por la derecha de R se verifican las tres condiciones. Veamos el recíproco: (iii) implica que el producto es una operación interna en I. Por otro lado, dado $y \in I$ y $0 \in R$, $0y \in I$ si I es un ideal por la izquierda ($0 = y0 \in I$ si I es un ideal por la derecha). Lo que demuestra que, en ambos casos, I es un subanillo de R. ■

Nos va a interesar construir ideales (por la izquierda, por la derecha) a partir de elementos. El siguiente teorema nos dice como.

Proposición 3 Sea R un anillo y $x \in R$. Entonces:

(i) $Rx = \{ax \mid a \in R\}$ es un ideal por la izquierda de R (si R es unitario $x \in Rx$).

(ii) $Rx + \mathbb{Z}x$ es un ideal por la izquierda de R que contiene a x. Es más, éste es el ideal por la izquierda más pequeño de R que contiene a x.

(i') $xR = \{xa \mid a \in R\}$ es un ideal por la derecha de R (si R es unitario $x \in xR$).

(ii') $xR + \mathbb{Z}x$ es un ideal por la derecha de R que contiene a x. Es más, éste es el ideal por la derecha más pequeño de R que contiene a x.

(iii) $RxR = \{\sum_{i=1}^{n} a_i x b_i \mid n \in \mathbb{N}, a_i, b_i \in R\}$ es un ideal de R (si R es unitario, $x \in RxR$).

(iv) $RxR + Rx + xR + \mathbb{Z}x$ es un ideal de R que contiene a x. Es más, éste es el ideal más pequeño de R que contiene a x.

Demo: Demostremos las tres propiedades necesarias dadas en el lema 2 (Pag. 102).

(i). $0 = 0x \in Rx$, por lo que es un conjunto no vacío. Veamos que la suma es interna: dados $ax, bx \in Rx$ tenemos que $ax + bx = (a + b)x \in Rx$. Veamos que los opuestos de elementos de Rx están en Rx: dado $ax \in Rx$, su opuesto es $(-a)x \in Rx$. Por último, dado $ax \in Rx$ y $b \in R$ tenemos que $b(ax) = (ba)x \in Rx$. Por lo que es un ideal por la izquierda de R.

(ii). $0 = 0x \in Rx + \mathbb{Z}x$, por lo que es un conjunto no vacío. Veamos que la suma es interna: dados $ax + \lambda x, bx + \mu x \in Rx + \mathbb{Z}x$ tenemos que

$$(ax + \lambda x) + (bx + \mu x) = (a + b)x + (\lambda + \mu)x \in Rx + \mathbb{Z}x.$$

Veamos que los opuestos de elementos de $Rx + \mathbb{Z}x$ están en $Rx + \mathbb{Z}x$: dado $ax + \lambda x \in Rx + \mathbb{Z}x$, su opuesto es $(-a)x + (-\lambda)x \in Rx + \mathbb{Z}x$. Por último, dado $ax + \lambda x \in Rx + \mathbb{Z}x$ y $b \in R$ tenemos que $b(ax + \lambda x) = (ba)x + (\lambda b)x \in Rx \subset Rx + \mathbb{Z}x$. Por lo que es un ideal por la izquierda de R.

(i') y (ii') se demuestran de forma análoga (ejercicio).

(iii). Es claro que $\emptyset \neq RxR$, ya que $0 = 0x0 \in RxR$. Por construcción la suma en RxR es interna. Es más, dado $\sum_{i=1}^{n} a_i x b_i \in RxR$ tenemos que su opuesto es $\sum_{i=1}^{n} (-a_i) x b_i$. Por último, dado $c \in R$ y $\sum_{i=1}^{n} a_i x b_i \in RxR$ tenemos que

$$c \cdot \sum_{i=1}^{n} a_i x b_i = \sum_{i=1}^{n} (c \cdot a_i) x b_i \in RxR$$
$$\sum_{i=1}^{n} a_i x b_i \cdot c = \sum_{i=1}^{n} a_i x (b_i \cdot c) \in RxR$$

Lo que demuestra que RxR es un ideal de R.

(iv). Denotemos por $I = RxR + Rx + xR + \mathbb{Z}x$. Es claro que $x \in I$, por lo que es no vacío. Por otro lado, dados $z = \sum_{i=1}^{n} a_i x b_i + cx + xd + \lambda x$ y $z' = \sum_{i=1}^{m} a'_i x b'_i + c'x + xd' + \lambda' x$ dos elementos de I tenemos que

$$z + z' = (\sum_{i=1}^{n} a_i x b_i + cx + xd + \lambda x) + (\sum_{i=1}^{m} a'_i x b'_i + c'x + xd' + \lambda' x)$$
$$= (\sum_{i=1}^{n} a_i x b_i + \sum_{i=1}^{m} a'_i x b'_i) + (c + c')x + x(d + d') + (\lambda + \lambda')x \in I$$

Por lo que la suma es una operación interna en I. Por otro lado el opuesto de un elemento $z = \sum_{i=1}^{n} a_i x b_i + cx + xd + \lambda x \in I$ es $-z = \sum_{i=1}^{n} (-a_i) x b_i + (-c)x + x(-d) + (-\lambda)x \in I$.

Por último, veamos la propiedad de ideal: sea $z = \sum_{i=1}^{n} a_i x b_i + cx + xd + \lambda x \in I$ y $t \in R$,

$$t \cdot z = t \cdot (\sum_{i=1}^{n} a_i x b_i + cx + xd + \lambda x) = \sum_{i=1}^{n} (t \cdot a_i) x b_i + (t \cdot c)x + txd + (\lambda t)x \in RxR + Rx \subset I$$

$$z \cdot t = (\sum_{i=1}^{n} a_i x b_i + cx + xd + \lambda x) \cdot t = \sum_{i=1}^{n} a_i x (b_i \cdot t) + cxt + x(d \cdot t) + x(\lambda t) \in RxR + xR \subset I$$

Lo que demuestra que I es un ideal de R. ■

Proposición 4 Sea R un anillo e I_1, I_2 dos ideales (ideales por la izquierda, por la derecha) de R. Entonces:

(i) $I_1 \cap I_2$ es un ideal (ideal por la izquierda, por la derecha) de R.

(ii) $I_1 + I_2$ es un ideal (ideal por la izquierda, por la derecha) de R.

(iii) $I_1 \cdot I_2 := \{\sum_{i=1}^{n} y_i y_i' \mid n \in \mathbb{N}, y_i \in I_1, y_i' \in I_2\}$ es un ideal (ideal por la izquierda, por la derecha) de R.

Es más, si I_1, I_2 son ideales de R, para $k = 1, 2$

$$I_1 I_2 \subset I_1 \cap I_2 \subset I_k \subset I_1 + I_2.$$

Demo: Vamos a dar las demostraciones suponiendo que I_1 e I_2 son dos ideales por la izquierda. Las demostraciones para ideales por la derecha o ideales son análogas (ejercicios). Vamos a demostrar que cada uno de estos subconjuntos verifican las tres condiciones del lema 2 (Pag. 102).

(i). ⋆ Demostremos que la suma es una operación interna en $I_1 \cap I_2$: dados $z, t \in I_1 \cap I_2$ tenemos que

$$\begin{aligned} z, t \in I_1 \quad & \text{por tanto como } I_1 \text{ es un subanillo, } z + t \in I_1. \\ z, t \in I_2 \quad & \text{por tanto como } I_2 \text{ es un subanillo, } z + t \in I_2. \end{aligned}$$

Luego $z + t \in I_1 \cap I_2$.

⋆ Dado $a \in R$, $y \in I_1 \cap I_2$ tenemos que

$$\begin{aligned} a \cdot y \in I_1 \quad & \text{al ser } I_1 \text{ ideal por la izquierda de } R. \\ a \cdot y \in I_2 \quad & \text{al ser } I_2 \text{ ideal por la izquierda de } R. \end{aligned}$$

Luego $a \cdot y \in I_1 \cap I_2$.

⋆ Dado $y \in I_1 \cap I_2$, $y \in I_1$ por lo que $-y \in I_1$ (al ser ideal por la izquierda) de igual modo, $-y \in I_2$ y por tanto $-y \in I_1 \cap I_2$.

(ii). ⋆ Demostremos que la suma es una operación interna en $I_1 + I_2$: sean $z, z' \in I_1 + I_2$, entonces existen $y_1, y_1' \in I_1$ e $y_2, y_2' \in I_2$ tales que $z = y_1 + y_2$ y $z' = y_1' + y_2'$. Por tanto

$$z + z' = y_1 + y_2 + y_1' + y_2' = (y_1 + y_1') + (y_2 + y_2') \in I_1 + I_2$$

⋆ Dados $a \in R$, y $z \in I_1 + I_2$, existen $y_1 \in I_1$ y $y_2 \in I_2$ tales que $z = y_1 + y_2$ y por tanto

$$a \cdot z = a \cdot (y_1 + y_2) = a \cdot y_1 + a \cdot y_2 \in I_1 + I_2$$

Ya que $a \cdot y_1 \in I_1$, al ser I_1 un ideal por la izquierda de R y $a \cdot y_2 \in I_2$, al ser I_2 ideal por la izquierda de R.

$\star$ Dado $z \in I_1 + I_2$, existen $y_1 \in I_1$ y $y_2 \in I_2$ tales que $z = y_1 + y_2$, por tanto

$$-z = -y_1 + (-y_2) \in I_1 + I_2$$

Ya que $-y_1 \in I_1$, al ser I_1 un ideal por la izquierda de R y $-y_2 \in I_2$, al ser I_2 ideal por la izquierda de R.

(iii). $\star$ Por la propia construcción de $I_1 \cdot I_2$ tenemos que la suma es interna aquí. Veamos las demás condiciones:

$\star$ Dado $a \in R$, $z \in I_1 \cdot I_2$, existen $y_i^1 \in I_1$, $y_i^2 \in I_2$, $i = 1, 2, \ldots, n$ tales que $z = \sum_{i=1}^n y_i^1 \cdot y_i^2$. Ahora,

$$a \cdot z = a \cdot \sum_{i=1}^n y_i^1 \cdot y_i^2 = \sum_{i=1}^n (a \cdot y_i^1) \cdot y_i^2 \in I_1 \cdot I_2$$

Ya que para todo $i = 1, 2, \ldots, n$, $a \cdot y_i^1 \in I_1$ y $y_i^2 \in I_2$.

$\star$ Dado $z \in I_1 \cdot I_2$, existen $y_i^1 \in I_1$, $y_i^2 \in I_2$, $i = 1, 2, \ldots, n$ tales que $z = \sum_{i=1}^n y_i^1 \cdot y_i^2$. Por tanto $-z = \sum_{i=1}^n (-y_i^1) \cdot y_i^2 \in I_1 \cdot I_2$. ■

Nota: Observar que para que $I_1 \cdot I_2$ sea ideal por la izquierda sólo hace falta que I_1 sea ideal por la izquierda.

Lema 5 [Ejercicio] Sea R un anillo e I un ideal (ideal por la izquierda, por la derecha) de R. Sea S un subanillo de R que contiene a I. Entonces I es un ideal (ideal por la izquierda, por la derecha)de S.

Teorema 6 (Segundo teorema de Isomorfía) Sea R un anillo e I_1, I_2 dos ideales de R. Entonces:

(i) I_1, I_2 son ideales de $I_1 + I_2$ y $I_1 \cap I_2$ es ideal tanto de I_1 como de I_2.

(ii) $I_1 + I_2/I_1 \approx I_2/(I_1 \cap I_2)$.

Demo: El apartado (i) se deduce del lema anterior. El apartado (ii) se demostrará haciendo uso del primer teorema de Isomorfía:

Por el apartado (i), I_1 es un ideal de $I_1 + I_2$, por lo que tiene sentido el anillo cociente $I_1 + I_2/I_1$. Por el apartado (i), $I_1 \cap I_2$ es ideal de I_2, por lo que tiene sentido el anillo cociente $I_2/(I_1 \cap I_2)$. Una vez que hemos demostrado que todos los anillos tienen sentido, demostremos el isomorfismo.

Consideremos la aplicación

$$f : I_2 \to I_1 + I_2/I_1 \quad \text{definida por} \quad f(y_2) = \overline{0 + y_2} \in I_1 + I_2/I_1.$$

Vamos a demostrar que f es un epimorfismo de anillos con $\mathrm{Ker}(f) = I_1 \cap I_2$. Tendremos entonces, aplicando el primer teorema de Isomorfía, que $R/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$, es decir, $I_2/(I_1 \cap I_2) \cong I_1 + I_2/I_1$.

• Es claro que f está bien definida, dado $y_2 \in I_2$, $f(y_2) = \overline{0+y_2}$ es un elemento de $I_1 + I_2/I_1$. Veamos que f es un homomorfismo de anillos. Sean $y_2, y_2' \in I_2$, tenemos entonces que

$$f(y_2 + y_2') = \overline{0 + (y_2 + y_2')} = \overline{0 + y_2'} + \overline{0 + y_2} = f(y_2) + f(y_2')$$
$$f(y_2 \cdot y_2') = \overline{0 + (y_2 \cdot y_2')} = \overline{0 + y_2'} \cdot \overline{0 + y_2} = f(y_2) \cdot f(y_2')$$

Luego es un homomorfismo de anillos.

Antes de demostrar el carácter sobreyectivo veamos una propiedad en el anillo cociente $I_1 + I_2/I_1$: para todo $y_1 \in I_1$ e $y_2 \in I_2$ se tiene que

$$\overline{y_1 + y_2} = \overline{0 + y_2} \quad \text{en} \quad I_1 + I_2/I_1 \tag{P}$$

Ya que $y_1 + y_2 - y_2 = y_1 \in I_1$.

• Veamos que es sobreyectivo: Dado $\overline{y_1 + y_2} \in I_1 + I_2/I_1$, tenemos que $\overline{y_1 + y_2} = \overline{0 + y_2}$ en $I_1 + I_2/I_1$. Por tanto,

$$f(y_2) = \overline{0 + y_2} = \overline{y_1 + y_2}$$

• Demostremos que $\mathrm{Ker}(f) = I_1 \cap I_2$. Vamos a demostrarlo por contenidos:

Sea $y \in I_1 \cap I_2$, tenemos entonces que

$$f(y) = \overline{0 + y} = \overline{y + 0} = \overline{0 + 0} = \overline{0} \quad \text{(propiedad (P))}$$

por lo que $I_1 \cap I_2 \subset \mathrm{Ker}(f)$.

Sea $y \in \mathrm{Ker}(f) \subset I_2$. Tenemos entonces que $\overline{0} = f(y) = \overline{0 + y}$, por tanto $0 + y - 0 \in I_1$ y por tanto $y \in I_1 \cap I_2$. ■

Definición 7 Recordamos que dado un anillo R, tanto $\{0\}$ como R son ideales de R, llamados los ideales triviales. Se dice que un ideal I de un anillo R es no trivial si es distinto de éstos. Se dice que un anillo R es **simple** si los únicos ideales que posee son los triviales.

Proposición 8 Sea R un anillo e I un ideal (izquierda o derecha) de R. Entonces

(i) Si I contiene un elemento inversible de R, $I = R$.

(ii) Los únicos ideales de un anillo de división son los triviales, es decir, los anillo de división (en particular, los cuerpos) son simples.

Demo: Supongamos que I es un ideal por la izquierda, para ideales por la derecha o ideales la demostración es análoga.

(i). Sea $x \in I$ un elemento inversible de R. Tenemos entonces que $x^{-1} \in R$, por lo que al ser I un ideal por la izquierda, $1 = x^{-1}x \in I$. Repitiendo que I es ideal por la izquierda, dado $a \in R$ (arbitrario) $a = a \cdot 1 \in I$, por lo que $R \subset I$ (trivialmente $I \subset R$), por lo que $I = R$.

(ii). Si I es un ideal en un anillo de división, o $I = \{0\}$ o contiene un elemento no nulo de R, por lo tanto un elemento inversible de R y por el apartado (i), $I = R$. ■

Proposición 9 Sea R un anillo unitario. Las siguientes condiciones son equivalentes:

- R es un anillo de división.
- para todo $0 \neq a \in R$, $Ra = R$.
- para todo $0 \neq a \in R$, $aR = R$.

Demo: Demostremos $(i) \iff (ii)$. En caso $(i) \iff (iii)$ es análogo. Supongamos que R es un anillo de división, entonces dado $0 \neq x \in R$, Rx es un ideal por la izquierda de R que contiene a x, luego por la proposición anterior $Rx = R$.

Sea R un anillo unitario tal que para todo $0 \neq x \in R$, $Rx = R$. Entonces, dado $0 \neq a \in R$, $Ra = R$, por lo Ra contiene al elemento unidad de R, así, existe $b \in R$ tal que $ab = 1$. Como $b \neq 0$ podemos repetir este argumento para b y existe $c \in R$ con $bc = 1$. Por último,

$$c = 1 \cdot c = (ab)c = a(bc) = a \cdot 1 = a$$

por lo que b es inversible con inverso a y por tanto a es inversible. ■

Corolario 10 (Ejercicio) Un anillo conmutativo y unitario R es un cuerpo si y sólo si es simple (sólo posee los ideales triviales).

Hay ejemplos de anillos simples que no son de división:

Teorema 11 Sea R un anillo y $n \in \mathbb{N}$. Entonces $\mathcal{I}$ es un ideal de $\mathcal{M}_n(R)$ si y solo si $\mathcal{I} = \mathcal{M}_n(I)$ para I un ideal de R.

Demo: Sea I un ideal de R. Entonces $\mathcal{M}_n(I)$ es un ideal de $\mathcal{M}_n(R)$:
$\star$ $(\mathcal{M}_n(I), +)$ es un grupo abeliano: dados $(y_{ij})_{ij=1}^n, (y'_{ij})_{ij=1}^n \in \mathcal{M}_n(I)$,

- $(y_{ij})_{ij=1}^n + (y'_{ij})_{ij=1}^n = (y_{ij} + y'_{ij})_{ij=1}^n \in \mathcal{M}_n(I)$.
- $(0_{ij})_{ij=1}^n \in \mathcal{M}_n(I)$
- El opuesto de $(y_{ij})_{ij=1}^n$ es $(-y_{ij})_{ij=1}^n \in \mathcal{M}_n(I)$

$\star$ Veamos que es un ideal: dados $(y_{ij})_{ij=1}^n \in \mathcal{M}_n(I)$ y $(x_{ij})_{ij=1}^n \in \mathcal{M}_n(R)$,

- $(x_{ij})_{ij=1}^n (y_{ij})_{ij=1}^n = (\sum_{k=1}^n x_{ik}y_{kj})_{ij=1}^n \in \mathcal{M}_n(I)$, ya que $x_{ik}y_{kj} \in I$ para cualesquiera $i, j, k \in \{1, 2, \cdots, n\}$.
- $(y_{ij})_{ij=1}^n (x_{ij})_{ij=1}^n = (\sum_{k=1}^n y_{ik}x_{kj})_{ij=1}^n \in \mathcal{M}_n(I)$, ya que $y_{ik}yx_{kj} \in I$ para cualesquiera $i, j, k \in \{1, 2, \cdots, n\}$.

Sea ahora $\mathcal{I}$ un ideal de $\mathcal{M}_n(R)$. Veamos que existe un ideal I de R tal que $\mathcal{I} = \mathcal{M}_n(I)$: denotemos por e_{ij} la matriz de $\mathcal{M}_n(R)$ que tiene un uno en el lugar ij y ceros en el resto.
$\star$ Dada una matriz $A = (a_{ij})_{ij=1}^n \in \mathcal{M}_n(R)$, $A = \sum_{ij=1}^n e_{ii}Ae_{jj}$: sólo hay que darse cuenta que $e_{ii}Ae_{jj}$ es la matriz que tiene a a_{ij} en el lugar ij y ceros en el resto.
$\star$ Si $Y = (x_{ij})_{ij=1}^n \in \mathcal{I}$, y considero $x_{rs} \in R$ la coordenadas rs de esta matriz, entonces la matriz A que tiene a x_{rs} en el lugar $r's'$ y ceros en el resto pertenece a $\mathcal{I}$: solo hay que darse cuenta que $A = e_{r'r}(x_{rs})_{ij=1}^n e_{ss'}$.

Consideremos la aplicación

$$\pi_{11} : \mathcal{M}_n(R) \to R \quad \text{definida por} \quad \pi((x_{ij})_{ij=1}^n) = x_{11}.$$

y sea $I = \pi_{11}(\mathcal{I})$ (el conjunto de las coordenadas 11 de cada matriz de $\mathcal{I}$).

Veamos que $\mathcal{I} \subset \mathcal{M}_n(I)$: dado $Y \in \mathcal{I}$, por la propiedad segunda, cada coordenada de Y pertenece a I.

Veamos que $\mathcal{M}_n(I) \subset \mathcal{I}$: dada una matriz $A \in \mathcal{M}_n(I)$, por la propiedad primera, $A = \sum_{ij=1}^{n} e_{ii}Ae_{jj}$ y por la propiedad segunda cada matriz $e_{ii}Ae_{jj} \in \mathcal{I}$. ■

Corolario 12 Sea R un anillo simple y unitario. Entonces para cada $n \in \mathbb{N}$, $\mathcal{M}_n(R)$ es un anillo simple y unitario. En particular $\mathcal{M}_n(\mathbb{F})$ es simple (y no es un cuerpo o un anillo de división) para cada cuerpo $\mathbb{F}$.

4. Subcuerpo primo

En esta sección vamos a ver que todo cuerpo $\mathbb{F}$ contiene como subanillo a $\mathbb{Z}_p$ o a $\mathbb{Q}$. Más precisamente:

Teorema 1 *Sea $\mathbb{F}$ un cuerpo. Entonces:*

- *Si $\mathbb{F}$ tiene característica cero, $\mathbb{Q} \subset \mathbb{F}$.*
- *Si $\mathbb{F}$ tiene característica p, $\mathbb{Z}_p \subset \mathbb{F}$.*

A $\mathbb{Q}$ o $\mathbb{Z}_p$, con p un número primo, se les denomina los subcuerpos primos.

Demo: Sea la aplicación $f : \mathbb{Z} \to \mathbb{F}$ definida por $f(n) = 1 + \overset{n}{\cdots} + 1 = n1$. Claramente, f es un homomorfismo de anillos, es más:

$\star$ Si la característica de Δ es 0, f es un monomorfismo de anillos, por lo que aplicado la propiedad fundamental del cuerpo de fracciones de un dominio de integridad, tenemos que existe $\bar{f} : \mathbb{Q} \to \mathbb{F}$ un monomorfismo de anillos, por lo que se puede considerar $\mathbb{Q}$ contenido en $\mathbb{F}$.

$\star$ Si la característica de $\mathbb{F}$ es un número p, (que sabemos que es un número primo), $\mathrm{Ker}(f) = p\mathbb{Z}$ y por el primer teorema de Isomorfía

$$\mathbb{Z}_p \approx \mathbb{Z}/\mathrm{Ker}(f) \approx \mathrm{Im}(f) \subset \mathbb{F}.$$

lo que nos demuestra el teorema. ■

5. Ideales primos, ideales maximales

Empecemos este tema estudiando la relación entre los ideales de un anillo R y los ideales de cualquier cociente suyo R/I.

Teorema 1 Sea R un anillo y sea I un ideal de R. Entonces:

- Si J es un ideal de R con $I \subset J \subset R$, entonces

$$\overline{J} = \{\overline{x} \in R/I \mid x \in J\} \text{ es un ideal de } R/I$$

- Si $\mathcal{K}$ es un ideal de R/I, existe K un ideal de R con $I \subset K \subset R$ tal que $\mathcal{K} = \overline{K}$.

Es más, los item anteriores definen una aplicación biyectiva entre el retículo de los ideales de R/I y el retículo de los ideales de R que contienen a I.

$$\begin{array}{rccc} \Phi: & \{J \lhd R \mid I \subset J \subset R\} & \longrightarrow & \{\mathcal{K} \mid \mathcal{K} \lhd R/I\} \\ & J & \longmapsto & \overline{J} \end{array}$$

Demo: • Sea J un ideal de R con $I \subset J$ (realmente esta propiedad solo se usara para demostrar la inyectividad de la aplicación Φ). Demostremos que $\overline{J} = \{\overline{x} \in R/I \mid x \in J\}$ es un ideal de R/I.

⋆ Sean $x, y \in J$ y consideremos $\overline{x}, \overline{y} \in \overline{J}$. Tenemos entonces que $\overline{x} + \overline{y} = \overline{x+y} \in \overline{J}$.

⋆ $\overline{0} \in \overline{J}$ y dado $x \in J$, $\overline{x} \in \overline{J}$ tiene por opuesto $\overline{-x} \in \overline{J}$ (ya que $-x \in J$).

⋆ Sea $a \in R$ y $x \in J$ y consideremos $\overline{a} \in R/I$ y $\overline{x} \in J$. tenemos entonces que $\overline{ax}$ y $\overline{xa} \in \overline{J}$ ya que $ax, xa \in J$.

• Dado $\mathcal{K}$ un ideal de R/I consideremos $K = \{x \in R \mid \overline{x} \in \mathcal{K}\}$. Veamos que K es un ideal de R que contiene a I tal que $\overline{K} = \mathcal{K}$.

⋆ Veamos que la suma es interna en K: dados $x, y \in K$ tenemos que $\overline{x}, \overline{y} \in \mathcal{K}$, por tanto $\overline{x+y} = \overline{x} + \overline{y} \in \mathcal{K}$, lo que implica que $x + y \in K$.

⋆ Es claro que $0 \in K$ (ya que $\overline{0} \in \mathcal{K}$) y si $a \in K$, $\overline{-a} = -\overline{a} \in \mathcal{K}$, lo que implica que $-a \in K$.

⋆ Sea $a \in R$ y $x \in K$. Tenemos entonces que $\overline{a \cdot x} = \overline{a} \cdot \overline{x} \in \mathcal{K}$ y $\overline{x \cdot a} = \overline{x} \cdot \overline{a} \in \mathcal{K}$, lo que implica que $a \cdot x, x \cdot a \in K$.

⋆ Por último, si $x \in I$, $\overline{x} = \overline{0} \in R/I$ y por tanto $I \subset K$.

⋆ Veamos que $\overline{K} = \mathcal{K}$. Si $\overline{x} \in \mathcal{K}$, por construcción de K tenemos que $x \in K$, por lo que $\overline{x} \in \overline{K}$. Por último, si $\overline{x} \in \overline{K}$, existe $y \in K$ tal que $\overline{x} = \overline{y} \in \mathcal{K}$.

Por último, veamos que la aplicación Φ es una aplicación biyectiva que conserva las inclusiones: El apartado primero nos dice que Φ está bien definida. El apartado segundo nos dice que Φ es sobreyectiva. Supongamos ahora que $\Phi(K) = \Phi(K')$, veamos que $K = K'$. Sea $x \in K$. Como $\overline{x} \in \Phi(K) = \Phi(K')$ existe $x' \in K'$ tal que $\overline{x} = \overline{x'}$, por lo que $x - x' \in I$ y por tanto $x = x' + y \in K'$. De forma similar se demuestra que un elemento de K' está contenido en K. ■

Nota: Normalmente, cuando tenemos R un anillo y tenemos $I \subset J$ dos ideales de R al ideal $\overline{J}$ de R/I se le suele representar por J/I (realmente son anillos isomorfos).

Teorema 2 (Tercer teorema de Isomorfía) Sea R un anillo e $I \subset J$ dos ideales de R. Entonces:

(i) J/I es un ideal de R/I.

(ii) $(R/I)/(J/I) \approx R/J$.

Demo: Por el lema 5 (Pag. 105) sabemos que I es un ideal de J y por la proposición anterior, como I es un ideal de R, $\overline{J} = J/I$ es un ideal de R/I, es decir, que todos los cocientes de (ii) tienen sentido. Al igual que el segundo teorema de Isomorfía, vamos a demostrarlo a partir del primer teorema de Isomorfía:

Consideremos las siguientes proyecciones canónicas: $\pi_1 : R \to R/I$ y $\pi_2 : R/I \to (R/I)/(J/I)$ y sea $f = \pi_2 \circ \pi_1$. Por tanto, $f : R \to (R/I)/(J/I)$ con $f(x) = \overline{\overline{x}}$. Por construcción, f es composición de dos homomorfismos sobreyectivos, por lo que es un homomorfismo sobreyectivo.

Veamos que $\mathrm{Ker}(f) = J$. Sea $x \in J$. Tenemos entonces que $f(x) = \overline{\bar{x}}$, pero $\overline{\bar{x}} = \overline{\bar{0}}$ ya que $\bar{x} - \bar{0} \in \overline{J} = J/I$. Por tanto, $x \in \mathrm{Ker}(f)$. Sea ahora $x \in \mathrm{Ker}(f)$. Tenemos entonces que $f(x) = \overline{\bar{x}} = \overline{\bar{0}}$, por tanto $\bar{x} - \bar{0} = \bar{x} \in J/I$, lo que implica que existe $y \in J$ con $\bar{x} = \bar{y}$ y por tanto $x - y = y' \in I$, por lo que $x = y + y' \in J$ (ya que $I \subset J$). Por tanto $\mathrm{Ker}(f) = J$.

En este momento sólo tenemos que aplicar el primer teorema de Isomorfía para demostrar que $R/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$, es decir, $R/J \cong (R/I)/(J/I)$. ■

Los dos últimos resultados importantes de este tema se van a centrar en teoría de anillos unitarios. No obstante las definiciones se harán de forma general.

Definición 3 Sea R un anillo. Se dice que un ideal I de R es maximal si $I \neq R$ y dado cualquier ideal J de R tal que $I \subset J \subset R$ se tiene que $J = I$ o $J = R$.

Teorema 4 Un ideal I de un anillo conmutativo y unitario R es maximal si y solo si el anillo cociente R/I es un cuerpo.

Demo: Supongamos que R/I es un cuerpo y sea J un ideal de R distinto de I con $I \subset J$. Entonces, dado $x \in J - I$, $\bar{0} \neq \bar{x} \in R/I$ y como R/I es un cuerpo, existe $\bar{z} \in R/I$ tal que $\overline{xz} = \overline{1}$. Por tanto, $xz - 1 = y \in I$ y así, $1 = xz - y \in J$, ya que $xz \in J$ y $y \in I \subset J$. Luego $J = R$ al contener a 1.

Supongamos que I es un ideal maximal de R y sea $\bar{0} \neq \bar{x} \in R/I$. Tenemos entonces que $x \notin I$. Por otro lado, Rx es un ideal de R que contiene a x (ya que R es conmutativo y unitario) y por tanto $I + Rx$ es un ideal de R que contiene a I y a x, por lo que, por la maximalidad de I, $I + Rx = R$. Así, existe $y \in I$ y $z \in R$ con $y + zx = 1$ o lo que es lo mismo, $\bar{x}\bar{z} = \bar{1}$ en R/I. Luego R/I es un anillo conmutativo y unitario en donde todo elemento no nulo tiene inverso, R/I es un cuerpo. ■

Definición 5 Sea R un anillo. Se dice que un ideal I de R es primo si $I \neq R$ y para todos $x, y \in R$ tales que $xy \in I$ se tiene que $x \in I$ o $y \in I$.

Teorema 6 Un ideal I de un anillo conmutativo y unitario R es primo si y solo si el anillo cociente R/I es un dominio de integridad.

Demo: Supongamos que el anillo cociente R/I es un dominio de integridad y sean $x, y \in R$ con $xy \in I$. Tenemos entonces que $\overline{xy} = \overline{0}$ en el dominio de integridad R/I por lo que o $\bar{x} = \bar{0}$, y así $x \in I$ o $\bar{y} = \bar{0}$, y así $y \in I$.

Supongamos que I es un ideal primo de R. Veamos que el anillo cociente R/I es un dominio de integridad. Sean $\bar{x}, \bar{y} \in R/I$, con $\bar{x}\bar{y} = \bar{0}$. Entonces $\overline{xy} = \bar{0}$ y por tanto $xy \in I$. Luego $x \in I$, y así $\bar{x} = \bar{0}$ o $y \in I$, y así $\bar{y} = \bar{0}$. Así, R/I es un anillo conmutativo y unitario sin divisores de cero. ■

Corolario 7 Sea R un anillo conmutativo y unitario. Entonces todo ideal maximal de R es primo.

Demo: Si I es un ideal maximal de R, R/I es un cuerpo y por tanto un dominio de integridad, lo que implica que I es un ideal primo. ■

6. Ejercicios del Tema

1 Sea R un anillo y $\approx$ una relación de equivalencia en R tal que en el conjunto cociente $R/\approx$ las siguientes operaciones están bien definidas.

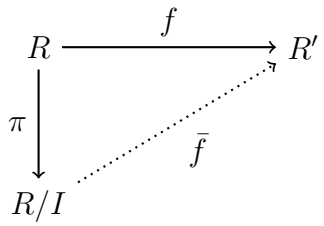
$$\overline{x} + \overline{y} := \overline{x+y} \qquad \overline{xy} := \overline{xy}.$$

Entonces, $(R/\approx, +, \cdot)$ tiene estructura de anillo.

2 Sean R y R' dos anillos, I un ideal de R y $f : R \to R'$ un homomorfismo de anillos. Demuestra que las siguientes condiciones son equivalentes:

(i) $I \subset \mathrm{Ker}(f)$.

(ii) Existe un único homomorfismo de anillos $\bar{f} : R/I \to R'$ que hace conmutativo el siguiente diagrama:



3 Demuestra que todo anillo unitario R posee ideales maximales:

(i) Demuestra, aplicando el lema de Zorn, que hay elementos maximales en la familia de los ideales de R que no contienen al 1.

(i) Demuestra que un ideal de esta familia es maximal en R

4 Sea R in anillo e I un ideal (ideal por la izquierda, por la derecha) de R. Sea S un subanillo de R que contiene a I. Entonces I es un ideal (ideal por la izquierda, por la derecha) de S.

5 Un anillo conmutativo y unitario R es un cuerpo si y sólo si es simple (sólo posee los ideales triviales).

6 Demuestra que para todo $k \in \mathbb{N}$, $k\mathbb{Z}$ es un ideal de $\mathbb{Z}$. Es más, demuestra que si I es un ideal de $\mathbb{Z}$ existe $n \in \mathbb{N}$ tal que $I = n\mathbb{Z}$.

7 Sea R un anillo y sea I un ideal de R. Demuestra que el núcleo de la proyección canónica $\pi : R \to R/I$ es precisamente I.

8 Sea R un anillo y $x \in R$. Demuestra que

(i') $xR = \{xa \mid a \in R\}$ es un ideal por la derecha de R (si R es unitario $x \in xR$).

(ii') $xR + \mathbb{Z}x$ es un ideal por la derecha de R que contiene a x. Es más, éste es el ideal por la derecha más pequeño de R que contiene a x.

9 Sea R un anillo e I_1, I_2 dos ideales por la derecha de R. Demuestra que:

(i) $I_1 \cap I_2$ es un ideal por la derecha de R.

(ii) $I_1 + I_2$ es un ideal por la derecha de R.

(iii) $I_1 \cdot I_2 := \{\sum_{i=1}^{n} y_i y_i' \mid n \in \mathbb{N}, y_i \in I_1, y_i' \in I_2\}$ es un ideal por la derecha de R.

10 Sea R un anillo e I_1, I_2 dos ideales de R. Demuestra que:

(i) $I_1 \cap I_2$ es un ideal de R.

(ii) $I_1 + I_2$ es un ideal de R.

(iii) $I_1 \cdot I_2 := \{\sum_{i=1}^{n} y_i y_i' \mid n \in \mathbb{N}, y_i \in I_1, y_i' \in I_2\}$ es un ideal de R.

11 Sea R un anillo e I un ideal por la izquierda (resp. por la derecha) de R. Entonces

(i) Si I contiene un elemento inversible de R, $I = R$.

(ii) Los únicos ideales por la izquierda (resp. por la derecha) de un anillo de división son los triviales.

12 Sea R un anillo y sea I un ideal de R. Demuestra que I es un ideal maximal de R si y sólo si el anillo cociente R/I es simple.

13 ¿Existe algún ideal $\mathcal{I}$ de $\mathcal{R} := \mathcal{M}_2(\mathbb{Z})$ tal que el cociente $\mathcal{R}/\mathcal{I}$ sea un cuerpo? (demuestra que la matriz $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ es siempre un elemento no nulo del cociente)

14 Demuestra que en $\mathbb{Z}$ un ideal $I \neq \{0\}$, es primo si y sólo si es maximal. Encuentra un ideal primo de $\mathbb{Z}$ que no sea maximal.

Capítulo 6

Anillos de polinomios

Objetivos del capítulo

-
-
-

---

1. Anillos de polinomios sobre anillos arbitrarios

Aunque ya se han visto los anillos de polinomios sobre un anillo arbitrario R, ver Proposición 15 (Pag. 70). En este tema vamos a estudiar más en profundidad alguna de sus propiedades.

Proposición 1 (Recordatorio) *Sea R un anillo. Se define el anillo de series formales sobre R y se representa por $R[[X]]$ como:*

$$R[X] := \{f : \mathbb{N} \to R\} \quad \textit{supondremos en este caso que } 0 \in \mathbb{N}$$

con suma y producto dado por:

1. *Suma:* $(f+g)(k) := f(k) + g(k)$.
2. *Producto:* $(f.g)(k) := \sum_{i=0}^{k} f(i)g(k-i)$

Proposición 2 (Recordatorio) *Sea R un anillo. Se define el anillo de polinomios con coeficientes en R, y se denota por $R[X]$ como el subanillo de $R[[X]]$,*

$$R[X] := \{f : \mathbb{N} \to R \mid f(i) = 0 \textit{ casi para todo } i\}$$

Aunque ésta es la definición formal de anillo de polinomios, normalmente se representan como:

$$R[X] := \{a_0 + a_1X + \cdots a_nX^n \mid n \in \mathbb{N},\ a_i \in R\}$$

En donde $p(X) = a_0 + a_1X + \cdots a_nX^n$ nos representa la función $f : \mathbb{N} \to R$ definida por

$$f(k) := \begin{cases} a_k, & k \leq n \\ 0, & k > n \end{cases}$$

Definición 3 *Sea R un anillo y $R[X]$ el anillo de polinomios con coeficientes en R. Dado $p(X) = a_0 + a_1X + \cdots a_nX^n \in R[X]$ se dice que los a_i son los coeficientes del polinomio siendo, a_k, el coeficiente que acompaña a X^k el coeficiente k-ésimo de $p(X)$. Se define el grado de un polinomio no nulo $p(X) \in R[X]$ y se representa por $\mathrm{dg}(P(X))$ como el mayor $k \in \mathbb{N}$ tal que $a_k \neq 0$. Se dice que un polinomio es constante si tiene grado cero. Se dice que un polinomio es mónico si su coeficiente de mayor grado es 1.*

Nota: Observar que, por construcción, dos polinomios son iguales si y sólo si coinciden coeficiente a coeficiente.

Proposición 4 *Sea R un anillo. Entonces:*

1. *Si R es unitario, $R[X]$ es unitario.*
2. *Si R es conmutativo, $R[X]$ es conmutativo.*
3. *Si $p(X), q(X) \in R[X]$ y el coeficiente de mayor grado de $p(X)$ no es un divisor de cero, entonces*
$$\mathrm{dg}(p(X)) \cdot q(X)) = \mathrm{dg}(p(X)) + \mathrm{dg}(q(X)).$$
4. *Si R es un dominio de integridad:*
   a) *Si $p(X), q(X) \in R[X]$, entonces $\mathrm{dg}(p(X)) \cdot q(X)) = \mathrm{dg}(p(X)) + \mathrm{dg}(q(X))$.*
   b) *$R[X]$ es un dominio de integridad.*
   c) *Los elementos inversibles de $R[X]$ son los polinomios constantes $p(X) = a$ con $a \in \mathrm{Inv}(R)$*

Nota: Que el grado del producto sea la suma de los grados no tiene que darse. Así, si consideramos $\mathbb{Z}_6[X]$, el anillo de los polinomios con coeficientes en $\mathbb{Z}_6$ y consideramos $p(X) = 1 + 2X^2$, $q(X) = 1 + 3X^4$ tenemos que $p(X) \cdot q(X) = 1 + 2X^2 + 3X^4$ por lo que

$$\mathrm{dg}(p(X) \cdot q(X)) = 4 \neq 6 = \mathrm{dg}(p(X)) + \mathrm{dg}(q(X))$$

Al igual que en el caso de los enteros nos encontramos aquí con un algoritmo de la división para polinomios sobre anillos arbitrarios:

Teorema 5 (Algoritmo de la división) *Sea R un anillo y sea $p(X), q(X) \in R[X]$ supongamos que el coeficiente de mayor grado de $q(X)$ es inversible en R. Entonces existen dos únicos polinomios $c(X)$ y $r(X) \in R[X]$ tales que*

$$p(X) = c(X)q(X) + r(X) \quad \textit{con } r(X) = 0 \textit{ o } \mathrm{dg}(r(X)) < \mathrm{dg}(q(X))$$

2. Anillos de polinomios sobre anillos conmutativos.

En toda esta sección vamos a trabajar con anillos conmutativos, lo que nos va a permitir hablar de homomorfismo evaluación y factorización de polinomios.

Definición 1 *Sea R un anillo conmutativo y sea $R[X]$ el anillo de polinomios con coeficientes en R. Sea $a \in R$ y $p(X) = a_0 + a_1X + \cdots a_nX^n \in R[X]$. Se define la evaluación de $p(X)$ en a y se representa por $p(a)$ como:*

$$p(a) := a_0 + a_1a + \cdots a_na^n \in R$$

Teorema 2 *Sea R un anillo y sea $a \in R$. Entonces la aplicación*

$$\Phi_a : R[X] \to R \quad \textit{definida por } \Phi_a(p(X)) := p(a)$$

en un epimorfismo de anillos, llamado el homomorfismo de evaluación asociado al a.

Teorema 3 (Teorema del Resto) *Sea R un anillo conmutativo y unitario y sea $a \in R$. Sea $p(X) \in R[X]$. Entonces el resto de dividir $p(X)$ por $X - a$ es $p(a)$.*

Corolario 4 *Sea R un anillo conmutativo y unitario y sea $a \in R$. Entonces el núcleo del homomorfismo evaluación Φ_a es el ideal de $R[X]$ generado por $X - a$.*

Definición 5 *Sea R un anillo conmutativo y unitario y sea $p(X) \in R[X]$. Se dice que un elemento $a \in R$ es una raíz de $p(x)$ si $p(a) = 0$.*

Teorema 6 *Sea R un dominio de integridad. Entonces un polinomio $p(X) \in R[X]$ de grado n tiene a lo sumo n raíces distintas.*

3. Anillos de polinomios sobre cuerpos.

3.1. Cuerpos en general

Nos vamos a centrar en estudiar en esta sección los anillos de polinomios sobre un cuerpo $\mathbb{F}$. Por el momento sabemos que:

- $\mathbb{F}[X]$ es un dominio de integridad.
- Tenemos un algoritmo de la división para elementos de $\mathbb{F}[X]$.
- un polinomio $p(X) \in \mathbb{F}[X]$ es inversible si y sólo si es constante y no nulo.
- Para cada $a \in \mathbb{F}$ tenemos asociado un epimorfismo de anillos, el homomorfismo de evaluación, $\Phi_a : \mathbb{F}[X] \to \mathbb{F}$ con $\Phi_a(p(X)) = p(a)$.
- Un polinomio $p(X)$ de grado n tiene a lo sumo n raíces en $\mathbb{F}$.

Veamos que en este contexto también podemos dar un teorema de factorización (al igual que en el caso de $\mathbb{Z}$).

Definición 1 *Sea $\mathbb{F}$ un cuerpo y $\mathbb{F}[X]$ el anillo de polinomios con coeficientes en $\mathbb{F}$. Diremos que un polinomio $p(X) \in \mathbb{F}[X]$ es irreducible si:*

(i) $\mathrm{dg}(p(X)) \neq 0$.

(ii) Si $p(X) = r(X) \cdot s(X)$ *entonces* $\mathrm{dg}(s(X)) = 0$ *o* $\mathrm{dg}(R(X)) = 0$.

Nota: Los polinomios irreducibles irreducibles en $\mathbb{F}[X]$ van a jugar el papel de los números primos en $\mathbb{Z}$. En este caso la condición (i) nos dice que un irreducible no es cero o una unidad (recordar que los números primos son $|p| \geq 2$. La condición (ii) nos dice que si un polinomio es irreducible y es producto de dos polinomios, uno de ellos es inversible (y por tanto un elemento no nulo de $\mathbb{F}$).

Nos vamos a preocupar de dar distintos criterios a lo largo de la sección que nos asegure cuando un polinomio $p(X)$ es irreducible (problema que puede ser muy complicado para ciertos polinomios sobre ciertos cuerpos).

Teorema 2 (Primer criterio de irreducibilidad) *Sea $\mathbb{F}$ un cuerpo y $p(X) \in \mathbb{F}[X]$. Entonces:*

(i) Si $\mathrm{dg}(p(X)) = 1$, $p(X)$ *es irreducible.*

(ii) Si $p(X)$ *es irreducible con* $\mathrm{dg}(p(X)) > 1$, $p(X)$ *no tiene raíces sobre* $\mathbb{F}$.

(iii) Si $\mathrm{dg}(p(X)) = 2$ *o* 3, $p(X)$ *es irreducible si y sólo si no posee raíces en* $\mathbb{F}$.

3.2. Sobre el cuerpo de los complejos y de los reales

Por primera y única vez en esta asignatura vamos a enunciar y utilizar un resultado sin demostrarlo previamente. Dicho resultado se denomina, curiosamente, el Teorema Fundamental del álgebra. Es un resultado, fácil de entender, difícil de demostrar (curiosamente las demostraciones de este teorema suelen hacer uso de teorías procedentes del análisis matemático). En cualquier caso este resultado nos va a ser muy útil ya que va a permitir caracterizar los polinomios irreducibles sobre $\mathbb{C}$ y tener un amplio conocimiento sobres los polinomios irreducibles sobre $\mathbb{R}$.

Definición 3 *Se dice que un cuerpo $\mathbb{F}$ es algebraicamente cerrado si dado $p(x) \in \mathbb{F}[X]$ con $\mathrm{dg}(p(X) \geq 1$ se tiene que $p(X)$ tiene una raíz en $\mathbb{F}$.*

Teorema 4 (Teorema fundamental del álgebra) *El cuerpo de los complejos es algebraicamente cerrado.*

Corolario 5 *Sea $\mathbb{C}$ el cuerpo de los complejos. Entonces*

(i) Todo polinomio $p(X) \in \mathbb{C}[X]$ se factoriza como producto de polinomios de grado 1. Es decir, existen $a, \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ tales que

$$p(X) = a(X - \alpha_1)(X - \alpha_2) \cdot (X - \alpha_n)$$

en donde a es el coeficiente de mayor grado de $p(X)$ y $\alpha_1, \alpha_2, \ldots, \alpha_n$ son las raíces de $p(X)$ en $\mathbb{C}$.

(ii) Un polinomio $p(X) \in \mathbb{C}[X]$ es irreducible sobre $\mathbb{C}$ si y sólo si $\mathrm{dg}(p(X)) = 1$.

Esto nos da la posibilidad de describir los polinomios irreducibles sobre $\mathbb{R}$.

Corolario 6 *Sea $\mathbb{R}$ el cuerpo de los reales. Entonces*

(i) Todo polinomio $p(X) \in \mathbb{R}[X]$ se factoriza como producto de polinomios de grado 1 o 2. Es decir,

$$p(X) = a(X - \alpha_1) \cdots (X - \alpha_s)(X^2 + \beta_1 X + \gamma_1) \cdots (X^2 + \beta_r X + \gamma_r)$$

en donde a es el coeficiente de mayor grado de $p(X)$ y $\alpha_1, \alpha_2, \ldots, \alpha_k$ son las raíces de $p(X)$ en $\mathbb{R}$.

(ii) Un polinomio $p(X) \in \mathbb{R}[X]$ es irreducible si y sólo si

- $\mathrm{dg}(p(X)) = 1$ *o,*
- $\mathrm{dg}(p(X)) = 2$, $p(X) = \alpha X^2 + \beta X + \gamma$ *con* $\beta^2 - 4\alpha\gamma < 0$.

3.3. Sobre el cuerpo de los racionales

La situación sobre el cuerpo de los racionales es extremadamente más compleja. Como veremos, vamos a poder encontrar polinomios irreducibles sobre $\mathbb{Q}$ de cualquier grado. No obstante, veamos que unas cuantas cosas si que se pueden decir.

Nota: Observar que dado un polinomio $p(X) \in \mathbb{Q}[X]$ siempre podemos encontrar unos enteros $a, b_0, b_1, \ldots, b_n$ tales que

$$p(X) = a^{-1}(b_0 + b_1 X + \cdots + b_n X^n).$$

Simplemente podemos tomar a como el denominador común para todos los coeficientes racionales de $p(X)$. Es más, como las nociones que estamos tratando (raíces, irreducibilidad, etc) no dependen de trabajar con un polinomio $p(x)$ o con un múltiplo escalar suyo, $ap(X)$, en la mayoría de los enunciados podremos suponer que el polinomio en cuestión tiene coeficientes enteros.

Proposición 7 *Sea $p(X) = a_0 + a_1 X + \cdots a_n X^n \in \mathbb{Z}[X]$ y sean $a, b \in \mathbb{Z}$ tales que* $\mathrm{m.\,c.\,d}(a, b) = 1$. *Supongamos que $a/b \in \mathbb{Q}$ es una raíz de $p(X)$. Entonces a_0 es divisible por a y a_n es divisible por b.*

Proposición 8 *Sea $\mathbb{Z}$ el anillo de los enteros y sea $k \in \mathbb{Z}$. Entonces la aplicación $\Psi_k : \mathbb{Z}[X] \to \mathbb{Z}_k[X]$ con $\Psi(a_0 + a_1 X + \cdots + a_n X^n) = \overline{a_0} + \overline{a_1} X + \cdots + \overline{a_n} X^n$ es un epimorfismo de anillos.*

Nota: *Normalmente denotaremos por $\overline{p(X)}$ a la imagen de $p(X) \in \mathbb{Z}[X]$ por Ψ_k. Es decir, $\Psi_k(p(X)) := \overline{p(X)}$*

Teorema 9 (Lema de Gauss) *Sea $\mathbb{Z}$ el anillo de los enteros y sea $p \in \mathbb{Z}$ un número primo. Sean $g(X), h(X) \in \mathbb{Z}[X]$ y $f(X) = g(X) \cdot h(X)$. Supongamos que p divide a todos los coeficientes de $f(X)$. Entonces p divide a todos los coeficientes de $g(X)$ o p divide a todos los coeficientes de $h(X)$.*

Definición 10 *Sea $p(X) \in \mathbb{Z}(X)$ un polinomio. Se dice que $p(X) = g(X) \cdot h(X)$ es una factorización propia de $p(X)$ si $\mathrm{dg}(g(X)) \geq 1$ y $\mathrm{dg}(h(X)) \geq 1$.*

Teorema 11 *Sea $p(X) \in \mathbb{Z}[X]$. Entonces $p(X)$ es un polinomio irreducible en $\mathbb{Q}[X]$ si y sólo si no admite factorizaciones propias en $\mathbb{Z}[X]$.*

Teorema 12 (criterio de irreducibilidad modular) *Sea $\mathbb{Z}$ el anillo de los enteros y sea $0 \neq f(X) \in \mathbb{Z}[X]$. Supongamos que existe un número primo $p \in \mathbb{Z}$ tal que:*

- *p no divide al coeficiente de mayor grado de $f(X)$*
- *$\overline{f(X)}$ es un polinomio irreducible en $\mathbb{Z}_p[X]$.*

Entonces $f(X)$ es un polinomio irreducible sobre $\mathbb{Q}[X]$.

Teorema 13 (criterio de irreducibilidad de Eisenstein) *Sea $\mathbb{Z}$ el anillo de los enteros y sea $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ un polinomio de grado $n \geq 1$. Supongamos que existe un número primo $p \in \mathbb{Z}$ tal que:*

- *p no divide a a_n*
- *p divide a $a_0, a_1, \ldots, a_{n-1}$.*
- *p^2 no divide a a_0.*

Entonces $f(X)$ es un polinomio irreducible sobre $\mathbb{Q}[X]$.

3.4. Factorización de polinomios

En esta sub-sección vamos a ver que el anillo de polinomios sobre un cuerpo $\mathbb{F}$ se comporta, con respecto a la factorización, de forma bastante parecida que el anillo de los enteros $\mathbb{Z}$.

Vamos a empezar demostrando la existencia de un máximo común divisor en el anillo de polinomios $\mathbb{F}[X]$ con $\mathbb{F}$ un cuerpo.

Definición 14 *Sea $\mathbb{F}$ un cuerpo y $\mathbb{F}[X]$ el anillo de polinomios con coeficientes en F. Sean $p(X)$, $q(X)$ dos polinomios de $\mathbb{F}[X]$ con $p(X) \neq 0$. Se define el máximo común divisor de $p(X)$ y $q(X)$ en $\mathbb{F}[X]$ como un polinomio $d(X) \in \mathbb{F}[X]$ tal que:*

- *$d(X)$ es un polinomio mónico.*
- *$d(X)$ divide a $p(X)$ y a $q(X)$.*
- *Si $h(X) \in \mathbb{F}[X]$ divide a $p(X)$ y a $q(X)$, entonces $d(X)$ divide a $h(X)$.*

Proposición 15 *Sea $\mathbb{F}$ un cuerpo y $\mathbb{F}[X]$ el anillo de polinomios con coeficientes en F. Sean $p(X)$, $q(X)$ dos polinomios de $\mathbb{F}[X]$ con $p(X) \neq 0$. Entonces:*

(i) existe y el único el máximo común divisor de $p(X)$ y $q(X)$ que denotaremos por $\mathrm{m.c.d}(p(X), q(X))$.

(ii) Existen $r(X), s(X) \in \mathbb{F}(X)$ *tales que*

$$\text{m. c. d}(p(X), q(X)) = r(X) \cdot p(X) + s(X) \cdot q(X)$$

Proposición 16 *Sea* $\mathbb{F}$ *un cuerpo y* $\mathbb{F}[X]$ *el anillo de polinomios con coeficientes en* F*. Sean* $p(X), f_1(X), f_2(X), \ldots, f_n(X)$ *tales que* $p(X)$ *es irreducible sobre* $\mathbb{F}$ *y divide al producto* $f_1(X) \cdot f_2(X) \cdots f_n(X)$*. Entonces* $p(X)$ *divide a alguno de los* $f_i(X)$*.*

Teorema 17 (Teorema de factorización única) *Sea* $\mathbb{F}$ *un cuerpo y* $\mathbb{F}[X]$ *el anillo de polinomios con coeficientes en* F*. Entonces, dado un polinomio no constante* $f(X) \in \mathbb{F}[X]$ *existen unos únicos polinomios irreducibles y mónicos* $p_1(X), p_2(X), \ldots, p_k(X)$*, salvo el orden, tales que*

$$f(X) = a_n(p_1(X) \cdot p_2(X) \cdots p_k(X))$$

en donde a_n *es el coeficiente de mayor grado de* $f(X)$*.*

4. Ideales y cocientes en $\mathbb{F}[X]$

4.1. Ideales en $\mathbb{F}[X]$

En esta última sección del tema vamos a estudiar como son y que propiedades tienen los ideales del anillo de polinomios sobre un cuerpo $\mathbb{F}$. Como postre vamos a estudiar los anillos cocientes en $\mathbb{F}[X]$.

Recordamos que dado un elemento $p(X) \in \mathbb{F}[X]$, el ideal generado por $p(X)$ es,

$$< p(X) >= \{f(X) \cdot p(X) \mid f(X) \in \mathbb{F}[X]\} = \mathbb{F}[X] \cdot p(X)$$

es decir, el conjunto de todos los polinomios que son divisibles por $p(X)$. Llamado el ideal principal generado por $p(X)$.

Teorema 1 *Sea* $\mathbb{F}$ *un cuerpo y* $\mathbb{F}[X]$ *el anillo de polinomios con coeficientes en* F*. Sea* I *un ideal de* $\mathbb{F}[X]$*. Entonces existe un único polinomio* $p(X) \in \mathbb{F}[X]$ *mónico tal que* $I =< p(X) >$*. Es decir, todo ideal de* $\mathbb{F}[X]$ *es principal.*

Teorema 2 *Sea* $\mathbb{F}$ *un cuerpo y* $\mathbb{F}[X]$ *el anillo de polinomios con coeficientes en* F*. Sea* $I =< p(X) >$ *un ideal de* $\mathbb{F}[X]$*. Las siguientes condiciones son equivalentes:*

(i) $p(X)$ *es un polinomio irreducible de* $\mathbb{F}[X]$*.*

(ii) $\mathbb{F}[X]/I$ *es un cuerpo.*

(ii) I *es un ideal maximal de* $\mathbb{F}[X]$*.*

(ii) I *es un ideal primo de* $\mathbb{F}[X]$*.*

(ii) $\mathbb{F}[X]/I$ *es un dominio de integridad.*

4.2. Cocientes en $\mathbb{F}[X]$

Vamos a estudiar ahora como son los cocientes en $\mathbb{F}[X]$. Sea I un ideal de $\mathbb{F}[X]$ ¿Quien es $\mathbb{F}[X]/I$?. Sabemos que existe un único polinomio mónico $f(X) \in \mathbb{F}[X]$ tal que $I =< f(X) >$. Supongamos que $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$.

★ Veamos que todo polinomio de $\mathbb{F}[X]$ es congruente a un polinomio de grado menor que n modulo I. Es decir, que dado $p(X) \in \mathbb{F}[X]$ existe $q(X) \in \mathbb{F}[X]$ con $\mathrm{dg}(q(X) < n$ tal que $\overline{f(X)} \equiv \overline{q(X)}$ en $\mathbb{F}[X]/I$:

Demostremos, por inducción, que toda potencia de X mayor que n es congruente a un polinomio de grado menos que n modulo I. Tenemos que en el anillo cociente $\overline{0} \equiv \overline{f(X)} = \overline{X^n} + \overline{a_{n-1}X^{n-1}} + \cdots + \overline{a_1X} + \overline{a_0}$, por lo que

$$\overline{X^n} = -(\overline{a_{n-1}X^{n-1}} + \cdots + \overline{a_1X} + \overline{a_0}) \in \mathbb{F}[X]/I$$

Supongamos ahora que $X^{k-1} \equiv \overline{b_{n-1}X^{n-1}} + \cdots + \overline{b_1X} + \overline{b_0}$ modulo I. Entonces,

$$\begin{aligned} X^k &\equiv X \cdot X^{k-1} \equiv X \cdot (\overline{b_{n-1}X^{n-1}} + \cdots + \overline{b_1X} + \overline{b_0}) = \overline{b_{n-1}X^n} + \cdots + \overline{b_1X^2} + \overline{b_0X} \\ &\equiv -b_{n-1}(\overline{a_{n-1}X^{n-1}} + \cdots + \overline{a_1X} + \overline{a_0}) + b_{n-2}X^{n-1} + \cdots + \overline{b_1X^2} + \overline{b_0X} \end{aligned}$$

Por tanto tenemos que $\mathbb{F}[X]/I = \{\overline{q(X)} \mid \deg(q(X)) < n\}$. Es más, ningún polinomio de grado menor que n puede ser congruente a cero modulo I, por lo que en este conjunto todos los representantes son distintos. Por ultimo, la suma es componente a componente y el producto sigue las reglas anteriores (si en un producto alguna potencia es mayor que n, se sustituye por su congruente de grado menor).

Ejemplos A *Sea $\mathbb{R}$ es cuerpo de los reales y sea $p(X) = X^2 + 1 \in \mathbb{R}[X]$. Calculemos quien es $\mathbb{R}[X]/ < p(X) >$. En primer lugar, como $p(X)$ es un polinomio irreducible de $\mathbb{R}[X]$, El anillo cociente $\mathbb{R}[X]/ < p(X) >$ es un cuerpo.*

Los elementos de $\mathbb{R}[X]/ < p(X) >$ son de la forma $\{\overline{ax} + \overline{b} \mid cona, b \in \mathbb{R}\}$. La suma es componente a competente y el producto es

$$(ax + \overline{b}) \cdot (cx + d) = acX^2 + (ad + bc)X + bd \equiv (ad + bc)X + bd - ac$$

Ya que $\overline{X} \equiv -1$ modulo I. Por tanto este cociente no es mas que el cuerpo de los complejos.

5. Ejercicios del Tema

Capítulo 7

Algunos dominios de integridad

Objetivos del capítulo

-
-
-

---

1. Definiciones del tema

Hemos estudiado a lo largo del curso dos anillos de integridad: $\mathbb{Z}$, el anillo de los enteros, y $\mathbb{F}[X]$ con $\mathbb{F}$ un cuerpo, el anillo de polinomios con coeficientes en un cuerpo, que además de ser dominios de integridad tienen una propiedad muy curiosa: todo elemento se escribe "de forma única" como producto de "primos". En este tema vamos a estudiar dominios de integridad con esta propiedad, los dominios de factorización única.

Definición 1 *Sea D un dominio de integridad. Se dice que $u \in D$ es una unidad si u es un elemento inversible de D. Dados $a, b \in D$. Se dice que a divide a b y se representa $a|b$ si existe $c \in D$ tal que $b = ac$.*

Propiedades 2 *Sea D un dominio de integridad y sean $a, b, c \in D$. Entonces:*

(i) $a|a$.

(ii) Si $a|b$ *y* $b|c$, *entonces* $a|c$.

(iii) Si $a|b$ *y* $a|c$, *entonces* $a|xb + yc$ *para todo* $x, y \in \mathbb{Z}$.

Propiedades 3 *Sea D un dominio de integridad y sean $a, b \in D$. Las siguientes condiciones son equivalentes:*

(i) $a|b$ *y* $b|a$.

(ii) Existe $u \in D$ *una unidad tal que* $a = ub$.

(iii) $Da = Db$ *(El ideal generado por* a *coincide con el ideal generado por* b*).*

Definición 4 *Si* a, b *verifican las condiciones anteriores, se dice que* a *y* b *son asociados y se representa por* $a \sim b$*.*

Corolario 5 *Sea* D *un dominio de integridad. Entonces la relación* $\sim$ *es de equivalencia.*

Definición 6 *Sea* D *un dominio de integridad. Se dice que un elemento* $p \in D$ *es irreducible si:*

(i) p *no es una unidad ni es cero.*

(ii) Si $p = ab$ *con* $a, b \in D$*, entonces* a *o* b *es una unidad de* D*.*

Ejemplos A *Los números primos de* $\mathbb{Z}$ *o los polinomios irreducibles de* $\mathbb{F}[X]$*, con* $\mathbb{F}$ *un cuerpo, son irreducibles.*

Teorema 7 *Sea* D *un dominio de integridad y sea* $0 \neq p \in D$ *que no es unidad. las siguientes condiciones son equivalentes:*

(i) p *es irreducible.*

(ii) Si $d|p$*, entonces* d *es inversible o* $d \sim p$*.*

(iii) Si $p = ab$ *entonces* $p \sim a$ *o* $p \sim b$*.*

Corolario 8 *Sea* D *un dominio de integridad y sean* $a, b \in D$ *con* a *irreducible. Entonces si* $b \sim a$*,* b *es irreducible.*

Definición 9 *Se dice que un dominio de integridad verifica la condición de cadena ascendente (C.C.A.) para sus ideales principales si toda cadena de ideales principales,*

$$Da_1 \subset Da_2 \subset \cdots \subset Da_n \subset \cdots$$

es estacionaria. Es decir, existe $k \in \mathbb{N}$ *tal que* $Da_k = Da_{k+s}$ *para todo* $s \in \mathbb{N}$*.*

Teorema 10 *Sea* D *un dominio de integridad que satisface C.C.A. para sus ideales principales. Entonces todo elemento de* D *se puede escribir como producto de elementos irreducibles.*

2. Dominios de factorización única (DFU)

Definición 1 *Se dice que un dominio de integridad* D *es un dominio de factorización única si para todo elemento no nulo* $a \in D$*, con* a *no inversible se tiene:*

(i) a *se factoriza como producto de irreducibles.*

(ii) Si $a = p_1 \cdots p_r = q_1, \cdots q_s$ *con* p_i, q_i *irreducibles, entonces* $r = s$ *y existe* $\sigma \in S_r$ *(el grupo de permutaciones con* r *elementos) tal que* p_i *es asociado a* $q_{\sigma(i)}$ *para* $i = 1, 2, \ldots, r$*.*

Nota: Sabemos que $\mathbb{Z}$ y $\mathbb{F}[X]$ son DFU.

Definición 2 *Sea D un dominio de integridad. Se dice que un elemento $p \in D$ es primo si para todo par de elementos $a, b \in D$, si $p|ab$ entonces $p|a$ o $p|b$.*

Lema 3 *Sea D un dominio de integridad y sean $p, a_1, \ldots, a_n \in D$. Supongamos que p es primo y divide a $a_1 a_2 \cdots a_n$. Entonces existe $k \in \{1, 2, \ldots, n\}$ tal que $p|a_k$.*

Teorema 4 *En un dominio de integridad D los elementos primos son irreducibles. Es más, si D es un DFU, se tiene el recíproco.*

Teorema 5 *Sea D un dominio de integridad. Las siguientes condiciones son equivalentes:*

(i) D verifica CCA y todo elemento irreducible de D es primo.

(ii) D es un DFU.

Proposición 6 *Sea D un dominio de factorización única. Sea $a \in D$ que factoriza como producto de primos $a = p_1^{n_1} \cdots p_k^{n_k}$, con $n_i \in \mathbb{N}$. Entonces los divisores de a, salvo asociados, son de la forma $p_1^{m_1} \cdots p_k^{m_k}$, con $m_i \leq n_i$.*

Definición 7 *Sea D un DFU. y sean $a_1, a_2, \ldots, a_n \in D$.*

⋆ Se define el máximo común divisor de $a_1, \ldots, a_n$ y se representa por

$$m.c.d(a_1, a_2, \ldots, a_n)$$

a cualquier $d \in D$ con las siguientes propiedades:

(i) $d|a_i$ para $i = 1, 2, \ldots, n$.

(ii) Si $r|a_i$ para $i = 1, 2, \ldots, n$, entonces $r|d$.

⋆ Se define el mínimo común múltiplo de $a_1, \ldots, a_n$ y se representa por

$$\mathrm{M.\,C.\,M}(a_1, a_2, \ldots, a_n)$$

a cualquier $d' \in D$ con las siguientes propiedades:

(i) $a_i|d$ para $i = 1, 2, \ldots, n$.

(ii) Si $a_i|r$ para $i = 1, 2, \ldots, n$, entonces $d|r$.

Proposición 8 *El máximo común divisor y el mínimo común múltiplo, si existen, son únicos salvo asociados.*

Teorema 9 *Sea D un dominio de factorización única y sean $a_1, \ldots, a_n \in D$ no nulos ni unidades. Sean $p_1, \ldots, p_k$ elementos primos de D tales que para cada $i \in \{1, \ldots, n\}$, $a_i = p_1^{n_1^i} \cdots p_k^{n_k^i}$. Entonces:*

(i) $m.c.d(a_1, a_2, \ldots, a_n)$ consiste en el producto de los primos comunes con el menor exponente.

(ii) $\mathrm{M.\,C.\,M}(a_1, a_2, \ldots, a_n)$ consiste en el producto de los primos comunes y no comunes con el mayor exponente.

Por tanto, dados $a, b \in D$ no nulos ni unidades,

$$a\ b = m.c.d(a, b)\ \ \mathrm{M.\,C.\,M}(a, b).$$

Nota: El teorema de Bezout no se tiene que verificar para DFU.

Teorema 10 *Si D es un DFU, entonces $D[X]$ es un DFU.*

3. Dominios de ideales principales (DIP)

Sea D un dominio de integridad, o más generalmente, sea D un anillo conmutativo y unitario. Sabemos entonces que dado $a \in D$ el ideal generado por a es Da. (en un anillo arbitrario R es $< a >= RaR + Ra + aR + \mathbb{Z}a$).

Nota: Durante esta sección denotaremos indistintamente al ideal generado por a como Da o $< a >$.

Definición 1 *Se dice que un dominio de integridad D es un dominio de ideales principales (DIP) si todo ideal de D es principal, es decir, si I es un ideal de D, existe $a \in I$ tal que $I = Da$.*

Nota: Sabemos que $\mathbb{Z}$ y $\mathbb{F}[X]$ con $\mathbb{F}$ un cuerpo son dominios de ideales principales: Los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ para $n \in \mathbb{N}$ y si I es un ideal de $\mathbb{F}[X]$ y $p(x)$ es un polinomio de I con grado mínimo, entonces $I =< p(x) >$.

Proposición 2 *Todo DIP verifica CCA para sus ideales.*

Proposición 3 *En un DIP los elementos irreducibles son primos.*

Teorema 4 *Todo DIP es un DFU.*

Proposición 5 *Sea D un DIP y sean $a_1, \ldots, a_n \in D$ no nulos ni inversibles. Entonces:*

(i) $d = m.c.d(a_1, \ldots, a_n)$ *si y sólo si* $Da_1 + Da_2 + \cdots + Da_n = Dd$.

(ii) $d = \mathrm{M.C.M}(a_1, \ldots, a_n)$ *si y sólo si* $Da_1 \cap Da_2 \cap \cdots \cap Da_n = Dd$.

Nota: Como corolario de (i) se obtiene el teorema de Bezout para DIP (recordamos que no era cierto para DFU).

Teorema 6 *Sea D un DIP y sea $0 \neq p \in D$. Las siguientes condiciones son equivalentes:*

(i) *p es primo (que es lo mismo que irreducible).*

(ii) *Dp es un ideal maximal de D.*

(iii) *D/Dp es un cuerpo.*

(iv) *D/Dp es un dominio de integridad.*

(v) *Dp es un ideal primo de D.*

Corolario 7 *Si D es un DIP y I es un ideal no nulo de D, I es un ideal primo si y sólo si es maximal.*

Nota: En un dominio de integridad D, el ideal nulo es siempre primo y no tiene que ser maximal (sólo es maximal si D es un cuerpo).

4. Dominios euclídeos (DE)

Cuando trabajamos con $\mathbb{Z}$ o con $\mathbb{F}[X]$, el anillo de polinomios sobre un cuerpo $\mathbb{F}$, demostramos que verificaban el "algoritmo de la division". En esta sección vamos a estudiar dominios de integridad en los que existe, en cierta forma, un algoritmo de la división.

Definición 1 *Sea D un dominio de integridad. Se dice que D es un dominio euclídeo (DE) si existe una función $\delta : D^* \to \mathbb{N}^*$ tal que:*

(i) dados $a, b \in D$ con $b \neq 0$ existe $c, r \in D$ tales que $a = cb + r$ en donde $r = 0$ o $\delta(r) < \delta(b)$.

(ii) para todo par de elementos no nulos $a, b \in D$, $\delta(a) \leq \delta(ab)$.

Nota: $\mathbb{Z}$ es un dominio euclídeo en donde δ es el valor absoluto y $\mathbb{F}[X]$, el anillo de polinomios sobre un cuerpo $\mathbb{F}$ es dominio euclídeo en donde δ es la función grado.

Teorema 2 *Todo DE es un DIP.*

Teorema 3 (Algoritmo de Euclides) *En DE se verifica el algoritmo euclídeo. Es decir,*

$\star$ dados $a, b \in D$ no nulos, si $a = cb + r$, entonces $m.c.d(a, b) = m.c.d(b, r)$

Por tanto, la función Euclídea permite un método recursivo para calcular el máximo común divisor de dos elementos no nulos:

Sean a, b dos elementos no nulos de un dominio Euclídeo D. Aplicamos el algoritmo de la división a los elementos a, b,

$$\begin{aligned}
a &= c_1 b + r_1 && \text{Si} \quad r_1 \neq 0, \quad \delta(r_1) < \delta(b) \\
b &= c_2 r_1 + r_2 && \text{Si} \quad r_2 \neq 0, \quad \delta(r_2) < \delta(r_1) \\
r_1 &= c_3 r_2 + r_3 && \text{Si} \quad r_3 \neq 0, \quad \delta(r_3) < \delta(r_2) \\
&\vdots \\
r_n &= c_3 r_{n+1} + r_{n+2} && \text{Si} \quad r_{n+2} \neq 0, \quad \delta(r_{n+2}) < \delta(r_{n+1})
\end{aligned}$$

Como $\delta(b) > \delta(r_1) > \cdots > \delta(r_n) > \cdots$, existe un k tal que $r_k = 0$. Para este k se tiene que $r_{k-2} = c_k r_{k-1}$ y por la propiedad $\star$

$$m.c.d(a, b) = m.c.d(b, r_1) = \cdots = m.c.d(r_{k-2}, r_{k_1}) = m.c.d(c_k r_{k-1}, r_{k_1}) = r_{k-1}.$$

5. El anillo de los enteros de Gauss

En esta última sección vamos a estudiar una familia de anillos que aparecen al adjuntar a $\mathbb{Z}$ un elemento $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ (es decir, ω es solución del polinomio $X^2 - \omega^2 \in \mathbb{Z}[X]$).

Definición 1 *Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Consideremos el subanillo de $\mathbb{C}$ generado por $\mathbb{Z}$ y ω, denotado por $\mathbb{Z}[\omega]$. Es claro que tienes que contener a $\mathbb{Z}$, y a $\mathbb{Z}\omega$ y a sumas de estos elementos. Es fácil ver que no contiene elementos nuevos:*

$$\mathbb{Z}[\omega] = \{n + m\omega \quad | \quad n, m \in \mathbb{Z}\}$$

Nota: Dado $\xi \in \mathbb{C}$ consideremos el homomorfismo evaluación $\Phi_\xi : \mathbb{Z}[X] \to \mathbb{C}$ que a cada $p(x) \in \mathbb{Z}[X]$ le hace corresponder $p(\xi)$. Entonces $\Im\Phi_\xi \cong \mathbb{Z}[\xi] \cong \mathbb{Z}[X]/(\mathrm{Ker}(\Phi_\xi))$.

Lema 2 *Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Entonces:*

(i) $w \notin \mathbb{Q}$.

(ii) Si $n + m\omega = n' + m'\omega \in \mathbb{Z}[\omega]$, *entonces* $n = n'$ *y* $m = m'$.

Nota: Recordamos el anillo de los enteros de Gauss que corresponde a $\mathbb{Z}[i]$ con i la raíz imaginaria ($i^2 = -1$).

Definición 3 *Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Consideremos $\mathbb{Z}[\omega]$:*

$\star$ *Se define el conjugado de un elemento $n + m\omega \in \mathbb{Z}[\omega]$ y se representa por $(n + m\omega)^*$ como*

$$(n + m\omega)^* := n - m\omega.$$

$\star$ *Se define la norma de un elemento $n + m\omega \in \mathbb{Z}[\omega]$ y se representa por $N(n + m\omega)$ como*

$$N(n + m\omega) := n^2 - \omega^2 m^2.$$

Proposición 4 *Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Sean $a, b \in \mathbb{Z}[\omega]$, entonces:*

(i) $aa^* = a^*a = N(a) = N(a^*)$.

(ii) $(ab)^* = a^*b^*$ *y* $a^{**} = a$.

(iii) $N(ab) = N(a)N(b)$.

(iv) a *es una unidad de* $\mathbb{Z}[\omega]$ *si y sólo si* $N(a) = \pm 1$. *Además,* $a^{-1} = N(a)\, a^*$.

(v) $N(a) = 0$ *si y sólo si* $a = 0$.

(vi) Si $N(a)$ *es un primo de* $\mathbb{Z}$, *entonces* a *es irreducible en* $\mathbb{Z}[\omega]$.

Teorema 5 *Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Entonces $\mathbb{Z}[\omega]$ verifica la C.C.A para sus ideales principales. En particular todo elemento de $\mathbb{Z}[\omega]$ factoriza como producto de irreducibles.*

Teorema 6 *Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Supongamos que para cada $r, s \in \mathbb{Q}$ existen $n, m \in \mathbb{Z}$ tales que*

$$|(r - m) - \omega^2(s - n)| < 1$$

Entonces $\mathbb{Z}[\omega]$ es un dominio euclídeo, con función Euclídea $\delta(a) = |N(a)|$.

Corolario 7 *EL anillo de los enteros de Gauss es un dominio euclídeo.*

Nota: Las unidades de $\mathbb{Z}[i]$ son $\pm 1, \pm i$.

Estudiemos ahora cuales son los elementos irreducibles de $\mathbb{Z}[i]$. Ya sabemos que dado $a = n + mi \in \mathbb{Z}[i]$, si $N(a)$ es un número primo, a es irreducible.

En primer lugar podríamos pensar que todo primo de $\mathbb{Z}$ es primo en $\mathbb{Z}[i]$, pero es falso: $5 = (2 + i)(2 - i)$ (esta es la factorización de 5 como producto de primos).

Proposición 8 *Un número primo $p \in \mathbb{Z}$ es primo en $\mathbb{Z}[i]$ si y sólo si no se puede escribir como suma de dos cuadrados.*

Demo: Supongamos que p se puede escribir como suma de dos cuadrados, $p = n^2 + m^2$. Entonces

$$p = (n + mi)(n - mi)$$

en donde $n + mi, n - mi$ si son primos de $\mathbb{Z}[i]$ (ya que su norma es un número primo).

Supongamos que $p = (n + mi)(n' + m'i)$, en donde $n + mi$, $n' + m'i$ no son unidades. Podemos suponer n, m son primos entre si, entonces:

$$\begin{aligned} nn' - mm' &= p \qquad (*) \\ nm' + mn' &= 0 \end{aligned} \tag{7.1}$$

veamos varios casos:

$\star$ Si $n = 0$, entonces $p = mi\ (n' + m'i) = -mm' + mn'i$, por tanto $n' = 0$ y $p = -mm'$ implica que m o m' es ± 1 (al ser p primo) y $n + mi = \pm i$ o $n' + m'i = \pm i$ es inversible.

$\star$ Si $m = 0$ llegamos al mismo resultado.

$\star$ So n, m son no nulos, entonces $nm' = -mn'$, como $m.c.d(n, m) = 1$, n divide a n', por lo que $n' = \alpha n$, Así, por $(*)$, $nm' = -n'm = -\alpha nm$, por lo que $m' = -\alpha m$. Ahora por $(**)$, $p = nn' - mm' = \alpha n^2 + \alpha m^2 = \alpha(n^2 + m^2)$ y así, como p es un primo de $\mathbb{Z}$, o $n^2 + m^2 = 1$ con lo que $n + mi$ sería inversible, o $\alpha = \pm 1$ y $p = (n + mi)(n - mi) = n^2 + m^2$, una suma de cuadrados. ■

Lema 9 *Sea $p \in \mathbb{Z}$ un número primo tal que $p \equiv 1$ (Mod 4). Entonces la ecuación $x^2 + 1 = 0$ tiene solución en $\mathbb{Z}_p$.*

Demo: En caso contrario, no habría elementos en $\mathbb{Z}_p$ tales que $x^2 = -1$ y como $\mathbb{Z}_p$ es un cuerpo para cada $r \in \mathbb{Z}_p$ existiría $s \in \mathbb{Z}_p$ con $rs = -1$ (los podré reordenar a pares), luego si multiplico todos los elementos de $\mathbb{Z}_p^*$,

$$(p - 1)! \equiv (-1)^{(p-1)/2} \ (\text{Mod } p)$$

y como $p \equiv 1$ (Mod 4), $(p - 1)/2$ es par por lo que

$$(p - 1)! \equiv 1 \ (\text{Mod } p)$$

que contradice el teorema de Wilson $(p - 1)! \equiv -1$ (Mod p). ■

Teorema 10 *Sea $p \in \mathbb{Z}$ un número primo. Entonces p es irreducible en $\mathbb{Z}[i]$ si y sólo si $p \equiv 3$ (Mod 4).*

Demo: Supongamos que p es reducible. Entonces por el teorema anterior $p = n^2 + m^2$ con $n, m \in \mathbb{N}$. Si $p = 2$, $p \equiv 2$ (Mod 4) y si p es impar, n es par y m es impar o viceversa, podemos suponer n par, por lo que

$$p \equiv n^2 + m^2 \equiv 0 + 1^1 \equiv 1 \text{ (Mod 4)} \qquad \text{ó,}$$
$$p \equiv n^2 + m^2 \equiv 0 + 3^3 \equiv 1 \text{ (Mod 4)}$$

Supongamos ahora que p es irreducible y no es congruente con 3 módulo 4. Entonces,
$\star$ p no puede ser congruente con cero módulo 4 (ya que es primo).
$\star$ Si $p \equiv 2$ (Mod 4), $p = 2$ que es reducible, contradicción.
$\star$ Luego $p \equiv 1$ (Mod 4). Tenemos entonces que la ecuación $x^2 + 1 \equiv 0$ (Mod p) tiene solución por lo que existe $u \in \mathbb{Z}$ tal que $u^2 + 1$ es divisible por p, pero en $\mathbb{Z}[i]$, $u^2 + 1 = (u + i)(u - i)$ y como es primo, p dividiría a $u - i$ o a $u + i$, una contradicción. ■

Teorema 11 *Sea $z = n + mi \in \mathbb{Z}[i]$, el anillo de los enteros de Gauss. Entonces z es irreducible (y por tanto primo) si y sólo si se verifica una de las siguientes condiciones:*

(i) $N(z)$ es un número primo.

(ii) $z \in \mathbb{Z}$ es un número primo con $z \equiv 3$ (Mod 4) o asociado a éste.

Demo: Por los teoremas anteriores, los elementos que verifican (i) y (ii) son irreducibles. Supongamos ahora que $z \in \mathbb{Z}[i]$ es irreducible y consideremos $N(z)$. Factorizamos $N(z)$ como producto de primos de $\mathbb{Z}$ y si p es uno de estos primos y es reducible sobre $\mathbb{Z}[i]$ lo escribimos como $p = (n + mi)(n - mi)$ producto de primos por (i),(con $n^2 + m^2 = p$) luego como z divide a $N(z)$, y es primo tiene que dividir a alguno de estos y por tanto es (salvo equivalencia) uno de estos. ■

Ejemplos A *Veamos un proceso para factorizar un número de Gauss: Consideremos $n + mi \in \mathbb{Z}[i]$.*

$\star$ *Paso primero: calculamos la norma de z.*

$$N(z) = n^2 + m^2$$

$\star$ *Paso segundo: factorizamos en $\mathbb{Z}$ el número entero $N(z)$.*

$$N(z) = p_1^{n_1} \cdots p_k^{n_k}$$

$\star$ *Paso tercero: Factorizamos cada uno de los primos que aparecen.*

$\star$ *Paso final: Como $N(z) = zz^*$, y $\mathbb{Z}[i]$ es un dominio de factorización única, al ser un dominio euclídeo, de la factorización en primos de $N(z)$ sólo nos tenemos que quedar con los que corresponden a z (que son justamente la mitad).*

Nota: Si p_i está en la factorización de $N(z)$ y es primo de $\mathbb{Z}[i]$, por tanto $p_i \equiv 3$ (Mod 4), entonces debe de aparecer elevado a un número par.

6. Ejercicios del Tema

Bibliografía

[1] Frank Ayres and Lloyd Jaisingh. *Abstract Algebra*. McGraw-Hill, 2004.

[2] P.M. Cohn. *Algebra*. John Wiley& Sons, 1989.

[3] Juan de Burgos. *Curso de Álgebra y Geometría*. Alhambra Universidad, 1980.

[4] John B. Fraleigh. *A First Course in Abstract Algebra*. Addison-Wesley Publishing Company, 1982.

[5] Thomas W. Hungerford. *Algebra*. Springer, 1974.

[6] W. Keith Nicholson. *Introduction to Abstract Algebra*. John Wiley& Sons, 1999.

[7] J. Dorronsoro y E. Hernández. *Números, Grupos y Anillos*. Addison- Wesley, 1996.

Nomenclatura

$(X, *)$	Conjunto con operación binaria, página 49
$(X, \leq)$	conjunto ordenado, página 17
$-$	Diferencia, página 3
$=$	igualdad de aplicaciones, página 7
$=$	igualdad de conjuntos, página 2
$[x]$	clase de equivalencia de x, página 15
$\#X$	Cardinal de X, página 12
$\aleph_0$	aleph sub cero, página 22
$\aleph_1$	aleph sub uno, página 22
$\bigcap_{i\in I}$	Intersección indexada, página 6
$\bigcup_{i\in I}$	Unión indexada, página 6
$\cap$	intersección, página 3
$\mathrm{CoDom}(f)$	Codominio, página 7
$\cup$	Unión, página 3
$\mathrm{Dom}(f)$	Dominio, página 7
$\dot{n}$	múltiplo de n, página 14
$\emptyset$	conjunto vació, página 2
$\exists$	Existe, página 7
$\forall$	Para todo, página 7
Id_X	Aplicación identidad en X, página 7
$\iff$	si y sólo si, página 2
$\mathrm{Im}(f)$	imagen, página 8
$\in$	pertenece, página 2
$\mathrm{Inf}(Y)$	Ínfimo, página 18
$\leq$	relación menor o igual, página 13
$\mathbb{N}$	El conjunto de los números naturales, página 27
$\mathbb{Z}$	Los Números Enteros, página 29
$\mathrm{Max}(Y)$	Máximo, página 18
$\mathrm{m.\,c.\,d}(x, y)$	Máximo Común Divisor, página 31
$\mathrm{M.\,C.\,M}(x, y)$	mínimo común múltiplo, página 36
$\mathrm{Min}(Y)$	Mínimo, página 18
$\neq$	desigual, página 2
$\not\subset$	no contenido, página 2
$\notin$	no pertenece, página 2
$\overline{X}$	Complemento, página 4
$\overline{x}$	clase de equivalencia de x, página 15
$\Rightarrow$	implica, página 2
$\subset$	Contenido, página 2
$\subsetneq$	estrictamente contenido, página 2
$\mathrm{Sup}(Y)$	Supremo, página 18

$\triangle$	Diferencia simétrica, página 3
$\varphi(n)$	Función de Euler, página 40
$\|n\|$	Valor absoluto de $n \in \mathbb{Z}$, página 30
$\|X\|$	Cardinal de X, página 21
$\|$	tal (tales) que, página 7
$\mathbb{Z}_n$	Anillo de congruencias módulo n, página 37
$\{X_i\}_{i\in I}$	Conjuntos indexados, página 5
${}^{y}\|_{x}$	y divide a x, página 31
$a * b$	Operación binaria, página 49
$a \equiv b \pmod n$	a congruente con b módulo n, página 14
$a \mathcal{R} b$	a relacionado con b, página 13
a^{-1}	Inverso de a, (caso de que exista), página 51
$f(A)$	imagen de un subconjunto, página 8
$f : X \to Y$	Aplicación, página 7
f^{-1}	aplicación inversa, página 12
$g \circ f$	composición de aplicaciones, página 10
$X/\mathcal{R}$	Conjunto cociente, página 15
$X/_{\approx}$	Conjunto cociente, página 15
$x < y$	x menor estricto que y, página 29
$x > y$	x mayor estricto que y, página 29
$x \geq y$	x mayor o igual que y, página 29
$X \times Y$	Producto cartesiano, página 4
$\mathcal{P}$	partición, página 14
$\mathcal{P}(X)$	Partes de un conjunto, página 2
$\mathcal{R}_{\mathcal{P}}$	Relación de equivalencia asociada a una partición, página 15
$\mathcal{U}(M)$	Elementos inversibles de un monoide M, página 52

Índice alfabético