Álgebra I

Curso 2020/21

Índice

Chapter 1

El lenguaje de los conjuntos

Comenzamos el curso con una breve discusión de las nociones de teoría de conjuntos que jugarán un papel esencial en vuestra formación matemática.

> ***Su uso hoy día es fundamental para expresar de manera correcta los razonamientos y conceptos matemáticos.***

Fue Georg Ferdinand Ludwig Philipp Cantor (San Petersburgo, 1845 -1918) quien expuso originalmente la Teoría de Conjuntos, sobre la que David Hilbert (Königsberg, Prusia Oriental, 1862-1943) declara

> *"Cantor ha creado para los matemáticos un paraíso de pensamiento del cual ya nadie nos expulsará".*

Al tiempo, fijaremos el sentido de los símbolos matemáticos básicos, que seguro os son ya familiares: $\in$ (pertenece), $\forall$ (para todo), $\exists$ (existe), $|$ (tal que), $\vee$ (o), $\wedge$ (y), etc.

1.1 Sobre la teoría axiomática de conjuntos

La matemática es una ciencia totalmente abstracta. En contraposición con otras ciencias como pueden ser la física, la química o la biología, en matemáticas no hay forma de comprobar si un resultado es o no correcto. Esto hace que para realizar las matemáticas se establezca un contexto y en este contexto los matemáticos se pongan de acuerdo en que reglas o conceptos se dan por válidos.

Cantor propuso el contexto de "conjuntos" como el contexto básico en el que se establecen los axiomas y en el que se ha de desarrollar la matemática.

En el contexto de conjuntos hay dos nociones básicas:

- ***Conjunto***.
- ***Pertenece***.

Estas nociones básicas no se pueden definir pero si se deben entender. Además si aceptamos el contexto de conjuntos como aquel en el que vamos a desarrollar las matemáticas, sólo podremos hablar de conjuntos. Esto es: *Todo objeto matemático es un conjunto y cualquier enunciado debe estar basado en conjuntos y en la pertenencia.*

Una vez establecido el contexto en el que vamos a desarrollar las matemáticas, al ser esta una ciencia totalmente abstracta, necesitaremos establecer unas "*reglas del juego*" que nos permitan realizar nuestra ciencia.

Estas *reglas del juego* se conocen con el nombre de **Axiomas** y no tienen porqué ser aceptadas o estar fijadas de antemano. Los matemáticos tenemos que ponernos de acuerdo en los axiomas que vamos a aceptar. La única condición para aceptar estos axiomas será que ***no den lugar a contradicciones***.

Los matemáticos Ernst Friedrich Ferdinand Zermelo (Berlín, 1871-1953) y Abraham Halevi Fraenkel (Múnich 1891-1965) fijaron la axiomática más aceptada de teoría de conjuntos: *La axiomática de Zermelo-Fraenkel*.

Utilizaremos cualquier tipo de letra,

$$A, B, C, \cdots, X, Y, Z, \cdots a, b, c, \cdots, x, y, z, \cdots, \alpha, \beta, \gamma, \cdots$$

para expresar un conjunto.

Utilizaremos $\in$ para indicar pertenece. Así escribiremos por ejemplo:

Sea $x \in X$.

Cuyo significado será:

Sea x un elemento de X.

Y, por supuesto, tanto x como X, son conjuntos.

Comenzamos estableciendo un primer concepto: **El concepto de contenido:**

Diremos que el conjunto X está contenido en el conjunto Y, y lo indicaremos $X \subseteq Y$ si todo elemento que pertenece a X también pertenece a Y.

Simbólicamente escribiremos:

Definición 1.1.1. $X \subseteq Y \Leftrightarrow \forall x \in X, x \in Y$.

El concepto de contenido está perfectamente definido. No como ocurre con el concepto de pertenece, que es básico y espero entendáis aunque no lo hemos (no podemos) definido.

El segundo concepto que definimos es el de igualdad. Simbólicamente:

Definición 1.1.2. $X = Y \Leftrightarrow X \subseteq Y \wedge Y \subseteq X$.

Que leeremos: X es igual a Y si (y solo si) X está contenido en Y e Y está contenido en X.

Ya que estamos hablando de un concepto (el de conjunto) totalmente abstracto, no podemos probar la existencia de ningún conjunto. Con el primer axioma aceptaremos la existencia de un conjunto especial, aquel que no tiene elementos:

Axioma 1: $\exists X; \forall x, x \notin X$.

Hasta ahora tenemos dos definiciones (contenido e igualdad) y un axioma, con esto podemos dar nuestro primer teorema:

Teorema 1.1.3. *Si X es un conjunto que satisface el Axioma 1, entonces $X \subseteq Y$, para cualquier conjunto Y.*

La demostración de este axioma es algo especial y no siempre este tipo de demostraciones fue aceptado. Es una demostración *por reducción al absurdo*. Este tipo de demostraciones consiste en negar la hipótesis del teorema y llegar a una contradicción, es decir hemos de llegar a algo que contradiga nuestros axiomas (en nuestro caso sólo tenemos el Axioma 1).

Lo primero que tememos que saber es negar las hipótesis del Teorema 1.1.3.

Notemos que negar un enunciado del tipo:

$\forall Y$ se cumple bla, bla, bla.

Sería:

$\exists Y$ que no cumple bla,bla, bla.

Por tanto la negación de la hipótesis del Teorema 1.1.3 sería:

Si X es un conjunto que satisface el Axioma 1, entonces $\exists Y$ tal que $X \nsubseteq Y$.

Y la afirmación $X \nsubseteq Y$ nos diría que ha de existir un elemento $x \in X$ que no esté en Y. Lo que contradice la hipótesis de que X satisface el Axioma 1, ya que X no tiene elementos.

Una consecuencia (o corolario) inmediato de este Teorema 1.1.3 es que sólo existe un conjunto que satisfaga el Axioma 1. Que podemos enunciar como:

Corolario 1.1.4. *Existe un único conjunto que satisface el Axioma 1. Denotaremos a este conjunto como $\emptyset$ o también 0 y lo llamaremos conjunto vacío o cero.*

Demostración. Si X_1 y X_2 son dos conjuntos que satisfacen el Axioma 1. Como X_1 satisface el Axioma 1 el Teorema 1.1.3 implica $X_1 \subseteq X_2$. Por otro lado como X_2 también satisface el Axioma 1, el mismo teorema nos daría $X_2 \subseteq X_1$. De donde tenemos la igualdad. ■

Hacer un estudio profundo de la axiomática de conjuntos en estos momentos sería muy arriesgado, habría muchas posibilidades de que no entendiéramos mucho y por otro lado este no es el objetivo del curso. Vamos entonce algunas reglas (de forma intuitiva) que me permitan trabajar o construir conjuntos, estás reglas están totalmente formalizadas en los axiomas de Zermelo-Fraenkel.

¿Cómo podemos dar un conjunto?

La axiomática nos permite dar un conjunto de dos formas distintas:

- Por extensión.
- Por comprensión.

Daremos un conjunto X por **extensión** cuando especifiquemos todos los elementos de X. Por ejemplo, si ya conocemos otros conjuntos a, b, c, podremos dar un nuevo conjunto cuyos elementos son estos tres conjuntos. Indicaremos esto como:

$$X = \{a, b, c\}.$$

A partir del único conjunto que tenemos hasta ahora, el vacío $\emptyset$ o cero 0, podemos dar (por extensión) un nuevo conjunto:

$$1 = \{\emptyset\} = \{0\}.$$

Este conjunto tiene un sólo elemento que es el conjunto vacío. Ya disponemos de dos conjuntos $\emptyset$ y 1 y por tanto podemos dar (por extensión) otro nuevo conjunto, el que tiene a estos dos como elementos:

$$2 = \{0, 1\}.$$

Podemos ya construir infinitos conjuntos: $3 = \{0, 1, 2\}, 4 = \{01, 2, 3\}, \cdots$.

Sin embargo, **NO** podemos dar por extensión el conjunto

$$\mathbb{N} = \{0, 1, 2, 3, \cdots\},$$

Dar un conjunto por extensión significa dar o listar "*todos sus elementos*" es imposible listar todos los elementos de un conjunto infinito. No vale poner puntos suspensivos y quedarse tan pancho. Necesitaremos un nuevo axioma para poder hablar del conjunto de los números naturales.

Daremos un conjunto por **comprensión** cuanto tengamos una propiedad referente a los elementos de un conjunto ya dado X y nos quedemos con el conjunto de los elementos de X que tienen esa propiedad. Por ejemplo, suponer que hemos podido construir el conjunto $\mathbb{N}$ de los números naturales y que sabemos que significa que un número natural es par. Entonces podemos da por comprensión el conjunto P de los número naturales pares. Indicaremos esto de la siguiente forma:

$$P = \{x \in \mathbb{N}; x \text{ es par }\}.$$

El conjunto de las partes de un conjunto.

Si $A \subseteq S$ diremos que A es un subconjunto de S, de esta manera hemos indicado una propiedad:

Ser subconjunto.

La propiedad de ser subconjunto no está (en principio) referida a los elementos de un conjunto, la axiomática de conjuntos incluye un axioma que permite, dado un conjunto S, construir el conjunto de los subconjuntos de S. Este conjunto es llamado conjunto de las partes (o subconjuntos) de S y lo indicamos:

$$\mathcal{P}(S) = \{A; A \subseteq S\}.$$

Notemos que $\mathcal{P}(S)$ no está definido por comprensión ya que los elementos A en $\mathcal{P}(S)$ no son elementos de un conjunto ya definido. Esto es, para que pudiésemos dar $\mathcal{P}(S)$ por comprensión necesitaríamos un conjunto ?? (que no tenemos) de manera que

$$\mathcal{P}(S) = \{A \in ??; A \subseteq S\}.$$

Necesitamos un axioma que nos permita hablar del conjunto de las partes de un conjunto S.

Como consecuencia del Teorema 1.1.3 tenemos que:

$$\forall S, \emptyset \in \mathcal{P}(S),$$

por tanto $\mathcal{P}(S) \neq \emptyset$ ya que por lo menos tiene un elemento. Por otro lado siempre $S \subseteq S$ y por tanto también tenemos:

$$\forall S, S \in \mathcal{P}(S),$$

Así, podemos concluir que:

- $\forall S, \mathcal{P}(S) \neq \emptyset$ y
- si $S \neq \emptyset$ entonces $\mathcal{P}(S)$ tiene al menos dos elementos $\emptyset$ y S.

Operaciones con conjuntos.

Aunque la axiomática de conjuntos permite definir uniones e intersecciones de conjuntos cualesquiera, vamos a restringir (en un principio) estas construcciones a los subconjuntos de un conjunto dado.

Así A y B son subconjuntos de S, el subconjunto de S de elementos a tales que $a \in A$ y $a \in B$ es llamado la *intersección* de A y B. Lo denotamos por $A \cap B$. Este conjunto puede definirse por comprensión de la siguiente forma:

$$A \cap B = \{a \in S \mid a \in A \wedge a \in B\}.$$

Notar que hemos usado $\mid$ en lugar de ; en la definición anterior, esta notación también es usual.

Si $A \cap B = \emptyset$, entonces A y B se dicen *disjuntos*.

La unión $A \cup B$ de A y B es el subconjunto de elementos a tales que $a \in A$ o $a \in B$:

$$A \cup B = \{a \in S \mid a \in A \vee a \in B\}.$$

Una importante propiedad que relaciona estas operaciones entre subconjunto de $\mathcal{P}(S)$ es la siguiente.

Proposición 1.1.5 (Propiedad distributiva)**.** *Para cualesquiera subconjuntos $A, B, C \subseteq S$,*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Demostración. Probamos la primera y dejamos la segunda como ejercicio. Sea $a \in A \cap (B \cup C)$. Como $a \in B \cup C$, será $a \in B \vee a \in C$, y como $a \in A$ bien $a \in A \cap B \vee a \in A \cap C$. Se deduce que $a \in (A \cap B) \cup (A \cap C)$. Ahora, sea $a \in (A \cap B) \cup (A \cap C)$. Será $a \in (A \cap B) \vee a \in (A \cap C)$. En cualquier caso $a \in A \wedge a \in B \vee a \in C$. Entonces $a \in A \wedge a \in B \cup C$, o sea que $a \in A \cap (B \cup C)$. □

Intersecciones y uniones pueden ser definidas para un conjunto arbitrario de subconjuntos de un conjunto S. Sea $\Gamma \subseteq \mathcal{P}(S)$ un tal conjunto de subconjuntos. Entonces definimos su intersección

$$\bigcap_{A\in\Gamma} A = \{a \in S \mid a \in A \ \forall A \in \Gamma\}$$

y su unión

$$\bigcup_{A\in\Gamma} A = \{a \in S \mid \exists A \in \Gamma \mid a \in A\} \ .$$

Si Γ es finito, digamos $\Gamma = \{A_1, A_2, \ldots, A_n\}$, entonces escribimos también $\bigcap_{i=1}^n A_i$ o $A_1 \cap A_2 \cap \cdots \cap A_n$ para su intersección y, análogamente, $\bigcup_{i=1}^n A_i$ o $A_1 \cup A_2 \cup \cdots \cup A_n$ para su unión. Es fácil ver que las propiedades distributivas son válidas para intersecciones y uniones arbitrarias de subconjuntos: $B \cap \bigcup_{A\in\Gamma} A = \bigcup_{A\in\Gamma}(B \cap A)$, $B \cup \bigcap_{A\in\Gamma} A = \bigcap_{A\in\Gamma}(B \cup A)$.

Si $A \subseteq S$ es cualquier subconjunto, se define su *complementario* como

$$c(A) = \{a \in S \mid a \notin A\}.$$

(otras notaciones usuales para este son $\overline{A}$, $S - A$).

Algunas propiedades elementales son:

1. $c(\emptyset) = S$,
2. $c(S) = \emptyset$,
3. $A \cap c(A) = \emptyset$,
4. $A \cup c(A) = S$,
5. $c(c(A)) = A$.

Algo menos evidentes son las siguientes:

Proposición 1.1.6 (Morgan)**.**

$$c(\bigcap_{A\in\Gamma} A) = \bigcup_{A\in\Gamma} c(A), \tag{1.1}$$

$$c(\bigcup_{A\in\Gamma} A) = \bigcap_{A\in\Gamma} c(A). \tag{1.2}$$

Demostración. Probamos la primera. Sea $a \in c(\bigcap_{A\in\Gamma} A)$. Entonces $a \notin \bigcap_{A\in\Gamma} A$ y, por tanto, $\exists A \in \Gamma \mid a \notin A$ o, lo que es lo mismo, $\exists A \in \Gamma \mid a \in c(A)$. Por tanto, $a \in \bigcup_{A\in\Gamma} c(A)$. Supongamos ahora $a \in \bigcup_{A\in\Gamma} c(A)$. Entonces $\exists A \in \Gamma \mid a \in c(A)$ o, lo que es lo mismo, $\exists A \in \Gamma \mid a \notin A$. Pero entonces $a \notin \bigcap_{A\in\Gamma} A$ y, por tanto, $a \in c(\bigcap_{A\in\Gamma} A)$. ■

También se cumple:

Proposición 1.1.7. *Para cualesquiera dos subconjuntos $A, B \in \mathcal{P}(S)$,*

$$A \subseteq B \Leftrightarrow c(B) \subseteq c(A).$$

Demostración. Si $A \subseteq B$, y $a \notin B$, entonces $a \notin A$, luego $c(B) \subseteq c(A)$. Y recíprocamente, si $c(B) \subseteq c(A)$, entonces $A = cc(A) \subseteq cc(B) = B$. ■

Para subconjuntos $A, B \in \mathcal{P}(X)$, es usual también construir el subconjunto

$$A\backslash B = \{a \in A \mid a \notin B\} = A \cap c(B).$$

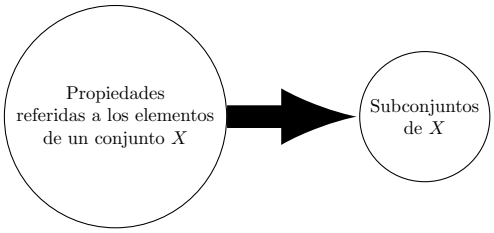
1.1.1 Proposiciones y Demostraciones.

Hemos aceptado que si tenemos una propiedad P referida a los elementos de un conjunto X podemos dar, por comprensión, el subconjunto de los elementos de X que tienen la propiedad P:

$$X_P = \{a \in X \mid a \text{ satisface } P\}.$$

Por ejemplo, si $\mathbb{Z}$ es el conjunto de los números enteros, entonces $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$ es el conjunto de los números naturales, o enteros no negativos.

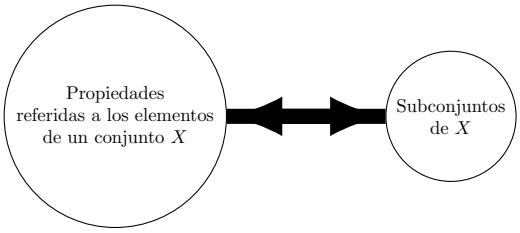
De esta manera podemos asociar a cada propiedad referida a los elementos de un conjunto X un elemento de $\mathcal{P}(X)$:



También podemos ir en sentido contrario. Esto es, a cada subconjunto $A \subseteq X$ le podemos asociar la propiedad referida a los elementos de X:

$P_A =$"ser elemento de A".

De manera que tenemos una equivalencia entre las propiedades referidas a los elementos de X y los subconjuntos de X.



Esta equivalencia nos permite trasladar conceptos de un contexto a otro. De manera que los operadores lógicos corresponden a operaciones en conjuntos. Así por ejemplo:

Si P y Q son propiedades referidas a los elementos de un conjunto X, la propiedad $P \wedge Q$, leída como *"P y Q"*, es aquella que es satisfecha exactamente por los elementos que satisfacen tanto P como Q. De manera que:

$$X_{P \wedge Q} = \{x \in X \mid x \in X_P \wedge x \in X_Q\} = X_P \cap X_Q$$

Decimos entonces que el conectivo lógico $\wedge$ equivale a la operación $\cap$.

Análogamente, la propiedad $P \vee Q$, leída como *"P o Q"*, se define como aquella que satisfacen exactamente los que satisfacen P o satisfacen Q. De forma que

$$X_{P \vee Q} = \{x \in X \mid x \in X_P \vee x \in X_Q\} = X_P \cup X_Q.$$

La propiedad que es verificada por aquellos elementos sobre los que una propiedad P es falsa, es denotada por $\neg P$, y leída como *"no P"*. Así que

$$X_{\neg P} = \{x \in X \mid x \notin X_P\} = c(X_P).$$

Operador lógico		Operación en conjuntos	
y	$\wedge$	$\cap$	intersección
o	$\vee$	$\cup$	unión
no	$\neg$	c	complementario

Table 1.1: Correspondencia operador lógico vs operación conjuntista

Podemos sintetizar esto en la siguiente Tabla 1.1.1:

Una *proposición matemática* es una relación entre dos propiedades P, Q referidas a los elementos de un conjunto X, del tipo $P \Rightarrow Q$, que leemos *"P implica Q"*, y significa que si un elemento de X satisface la propiedad P entonces ese elemento también satisface la propiedad Q.

Esto es:

La proposición $P \Rightarrow Q$ será verdad si $X_P \subseteq X_Q$.

Demostrar una proposición $P \Rightarrow Q$ consistirá precisamente en probar la inclusión $X_P \subseteq X_Q$.

La negación de este hecho que escribimos $P \not\Rightarrow Q$, significa entonces que $X_P \nsubseteq X_Q$, esto es que:

$$\exists a \in X_P;\ a \notin X_Q.$$

Así:

La falsedad de una proposición, se demuestra con un *contraejemplo.*

Una propiedad fundamental en el manejo de las proposiciones es la siguiente

Proposición 1.1.8 (Transitividad)**.** *Sean P, Q y R propiedades referidas a los elementos de un conjunto X. Si $P \Rightarrow Q$ y $Q \Rightarrow R$, entonces $P \Rightarrow R$.*

Demostración. Si $X_P \subseteq X_Q \subseteq X_R$, entonces $X_P \subseteq X_R$. ■

Cuando se satisface $P \Rightarrow Q$ y $Q \Rightarrow P$, decimos que las propiedades P y Q son*equivalentes.* Será por que $X_P = X_Q$.

Expresamos este hecho simbólicamente por $P \Leftrightarrow Q$, leído como:

Un elemento satisface P si y solo si satisface Q, o *P se satisface cuando y solo cuando Q lo hace.*

El siguiente hecho es un recurso muy utilizado en demostraciones.

Proposición 1.1.9. *Sean P_1, ..., P_n, una lista de propiedades referidas a los elementos de un conjunto X. Si se satisface que $P_1 \Rightarrow P_2$, $P_2 \Rightarrow P_3$, ..., $P_{n-1} \Rightarrow P_n$ y $P_n \Rightarrow P_1$, entonces $P_i \Leftrightarrow P_j$ para todo i, j.*

Demostración. Es consecuencia de la transitividad: Si $i < j$, tenemos que $P_i \Rightarrow P_j$ y también $P_j \Rightarrow P_1 \Rightarrow P_i$. ■

Proposición 1.1.10. *Para cualesquiera dos subconjuntos $A, B \in \mathcal{P}(X)$,*

$$A \subseteq B \Leftrightarrow c(B) \subseteq c(A).$$

Demostración. Si $A \subseteq B$, y $a \notin B$, entonces $a \notin A$, luego $c(B) \subseteq c(A)$. Y recíprocamente, si $c(B) \subseteq c(A)$, entonces $A = cc(A) \subseteq cc(B) = B$. ■

El siguiente hecho también es un recurso muy utilizado en demostraciones.

Proposición 1.1.11. *Sean P y Q propiedades referidas a elementos de un con junto X. Las siguientes proposiciones son equivalentes (en el sentido de que se satisface una si y solo si se satisface la otra, por tanto demostrar una es equivalente a demostrar la otra):*

(i) $P \Rightarrow Q$.

(ii) $\neg Q \Rightarrow \neg P$.

Demostración. $X_P \subseteq X_Q$ equivale a que $c(X_Q) \subseteq c(X_P)$. ■

Cuando uno demuestra $\neg Q \Rightarrow \neg P$ para probar $P \Rightarrow Q$, se dice que razonamos el ***contrarecíproco*** de la proposición original.

También se suele decir que demostramos $P \Rightarrow Q$ *por reducción al absurdo*: Supongamos que un elemento verifica P pero no Q. Entonces verifica $\neg Q$ y, por tanto, $\neg P$. Es decir, que no verifica P en contradicción a la hipótesis.

Ejercicios

En los siguientes enunciados, $A, B, C, ...$ refieren a subconjuntos arbitrarios de un conjunto dado X, y se pide demostrar la veracidad de las equivalencias o igualdades propuestas.

1. $A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$.

2. $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$.

3. (a) $A \cap B = \emptyset \Leftrightarrow A \subseteq c(B) \Leftrightarrow B \subseteq c(A)$.
   (b) $A \cup B = X \Leftrightarrow c(A) \subseteq B \Leftrightarrow c(B) \subseteq A$.

4. $(A - B) \cap (A - C) = A - (B \cup C)$.

5. (a) $A - B = A \Leftrightarrow A \cap B = \emptyset$.
   (b) $A \cap (B - C) = (A \cap B) - (A \cap C)$.

6. Siendo la "*diferencia simétrica*" $A \triangle B$ de A y B el subconjunto

$$A \triangle B = (A - B) \cup (B - A),$$

   (a) $A \triangle B = (A \cup B) - (A \cap B)$.
   (b) $A \triangle B = B \triangle C$.
   (c) $A \triangle \emptyset = A$.
   (d) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$
   (e) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

7. Si A y B son finitos, $|A \cup B| + |A \cap B| = |A| + |B|$.

8. Si A, B, y C son finitos,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

En los siguientes enunciados, $P, Q, R, ...$ refieren a propiedades que pueden ser satisfechas, o no, por los elementos de un conjunto X. Se pide demostrar la veracidad de las proposiciones o propuestas siguientes.

9. (a) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$.
   (b) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$.

10. Las siguientes proposiciones son equivalentes:
    (a) $P \Rightarrow Q$.
    (b) $P \vee Q \Leftrightarrow Q$.
    (c) $P \wedge Q \Leftrightarrow P$.

11. (a) $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$.
    (b) $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$.

12. $(P \vee \neg Q) \vee (P \vee \neg R) \Leftrightarrow P \vee \neg(Q \wedge R)$.

13. $P \vee Q \vee \neg Q \Leftrightarrow P \vee Q \vee \neg(P \vee R)$.

14. $(P \vee \neg Q) \wedge (Q \vee \neg P) \Leftrightarrow (P \wedge Q) \vee \neg(P \vee Q)$.

1.2 El conjunto producto cartesiano. Aplicaciones

Si S y T son conjuntos, su *producto cartesiano*, denotado $X \times Y$, es el conjunto de todos los pares ordenados (x, y) con $x \in S$ e $y \in T$:

$$S \times T = \{(x, y) \mid x \in S,\, y \in T\}.$$

En este conjunto, los elementos (x, y) y (x', y') son considerados iguales si y solo si $x = x'$ e $y = y'$. Así, si $|S| = m$ y $|T| = n$, entonces $|S \times T| = mn = |S|\,|T|$. Los conjuntos S y T no tienen que ser distintos. Cuando $S = T$, escribimos también S^2 en lugar de $S \times S$.

Más generalmente, desde n conjuntos dados listados en un cierto orden, S_1, ..., S_n, podemos formar el producto

$$S_1 \times S_2 \times \cdots \times S_n = \prod_{i=1}^{n} S_i = \{(x_1, x_2, \cdots, x_n) \mid x_i \in S_i \ \forall\, i = 1, \ldots, n\};$$

cuando $S_1 = S_2 = \cdots = S_n = S$ uno también escribe S^n en lugar de $S_1 \times S_2 \times \cdots \times S_n$.

Definición 1.2.1. *Una "aplicación" es una terna de datos (S, T, f), donde S es un conjunto, llamado el "dominio" de la aplicación, T es otro conjunto, llamado el "rango" de la aplicación, y $f \subseteq S \times T$ es un subconjunto del producto cartesiano, llamado su "grafo" , tal que las siguientes dos propiedades se verifican.*

1. *Para cualquier $x \in S$ existe un $y \in T$ tal que $(x, y) \in f$.*
2. *Si $(x, y), (x', y') \in f$, entonces $x = x' \Rightarrow y = y'$.*

Dos aplicaciones son consideradas iguales si y solo si tienen el mismo dominio, el mismo rango y los mismos grafos.

La notación usual para una tal aplicación es escribir $f : S \to T$ o $S \xrightarrow{f} T$, y uno se refiere a ella como *la aplicación f del conjunto S en el conjunto T* Las condiciones anteriores establecen que para cualquier elemento x del dominio hay un único elemento y del rango tal que (x, y) pertenece al grafo. La notación usual para ese elemento es $f(x)$, al que uno se refiere como la *imagen de x por f*, o *el elemento de T que corresponde a x por f*.

Para conocer una aplicación $f : S \to T$ es suficiente especificar la imagen $f(x)$ en T de cada elemento x de S. Usualmente, esto se hace proponiendo una fórmula que determina, para cada $x \in S$, su imagen $f(x) \in T$. Pero hay que ser cuidadoso en esto: Es necesario garantizarse que cada elemento de S tiene "bien definida su imagen" $f(x)$, esto es, que cada elemento S tiene una imagen y solo una.

Ejemplos.

1. Sea $\mathbb{N} = \{0, 1, 2, \ldots, \}$ el conjunto de los números naturales. No existe una aplicación $f : \mathbb{N} \to \mathbb{N}$ tal que la imagen de cada natural x venga dada por la fórmula $f(x) = x - 1$, pues el 0 no tiene asignado imagen. Esa fórmula, sin embargo si define una aplicación $f : \mathbb{Z} \to \mathbb{Z}$.

2. No existe una aplicación $f : \mathbb{N} \to \mathbb{N}$ tal que la imagen $f(x)$ de cada natural x venga dada por la fórmula

$$f(x) = \begin{cases} x & \text{si} \quad x \text{ no es múltiplo de 2 ni de 3} \\ x/2 & si \quad x \text{ es un múltiplo de 2,} \\ x/3 & si \quad x \text{ es un múltiplo de 3,} \end{cases}$$

pues hay naturales que corresponden a más de uno (es decir, con más de una imagen): $f(6) = 6/2 = 3$ y $f(6) = 6/3 = 2$. Esto es, los elementos $(6, 2)$ y $(6, 3)$ pertenecerían al grafo!.

3. Hay una aplicación $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $(m, n) \mapsto m + n$.

4. La correspondencia $x \mapsto f(x) = \frac{x^2+1}{x-1}$ define una aplicación $f : (0, 1) \to \mathbb{R}$, pero no una aplicación $f : [0, 1] \to \mathbb{R}$.

Usualmente, el subconjunto de todas las imágenes de una aplicación $f : S \to T$

$$Im(f) = \{y \in T \mid y = f(x) \text{ para algún } x \in S\} = \{f(x) \mid x \in S\}$$

es llamado la *imagen* de la aplicación.

La aplicación es llamada *sobreyectiva* is $Im(f) = T$, esto es, cuando todo elemento del rango es imagen de algún elemento del dominio.

La aplicación es llamada *inyectiva* si distintos elementos del dominio tienen distintas imágenes, esto es, si $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.

Si la aplicación f es simultáneamente inyectiva y sobreyectiva, entonces es llamada una *biyección*. Así, una aplicación $f : S \to T$ es una biyección cuando y solo cuando $\forall y \in T, \exists! x \in S \mid f(x) = y$. Si es posible establecer una biyección $f : S \to T$, se dice que S es biyectivo con T, y se expresa escribiendo $S \cong T$.

Ejemplos. Sea $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ el conjunto de los números enteros.

1. La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ tal que $f(x) = x^2$, no es inyectiva ni sobreyectiva.

2. La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ tal que $f(x) = 2x$, es injectiva pero no sobreyectiva.

3. La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ tal que $f(x) = x + 2$ es biyectiva.

4. Denotemos por $\mathbf{2} = \{0, 1\}$ al conjunto con dos elementos, y sea $\mathbf{2}^S$ al conjunto de todas las aplicaciones $f : S \to \mathbf{2}$. Si $A \in \mathcal{P}(S)$, se define su *aplicación característica* $\chi_A : S \to \mathbf{2}$ por
$$\chi_A(x) = \begin{cases} 1 & \text{si} \quad x \in A, \\ 0 & \text{si} \quad x \notin A. \end{cases}$$
La correspondencia $A \mapsto \chi_A$, nos define una aplicación biyectiva $\chi : \mathcal{P}(S) \cong \mathbf{2}^S$: Si $\chi_A = \chi_B$, entonces $A = \{x \in S \mid \chi_A(x) = 1\} = \{x \in S \mid \chi_B(x) = 1\} = B$, por tanto χ is inyectiva. Para ver que es sobreyectiva, supongamos $f : S \to \mathbf{2}$ cualquier aplicación. Sea $A = \{x \in S \mid f(x) = 1\}$. Entonces $\chi_A = f$, pues dado cualquier $x \in S$, si $f(x) = 1$ entonces $x \in A$ y $\chi_A(x) = 1$, y si $f(x) = 0$, entonces $x \notin A$ y también $\chi_A(x) = 0$.

Sean $S \xrightarrow{f} T$ y $T \xrightarrow{g} U$ dos aplicaciones, donde el rango de f coincide con el dominio de g, de manera que se pueden escribir consecutivamente como $S \xrightarrow{f} T \xrightarrow{g} U$. Se define su *composición* como la aplicación $S \xrightarrow{gf} U$, cuyo dominio es S, el rango es U y, para cualquier $x \in S$,

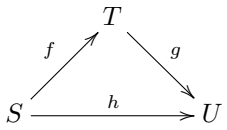
$$(gf)(x) = g(f(x)).$$

La composición de aplicaciones satisface la *ley asociativa*: Si $S \xrightarrow{f} T \xrightarrow{g} U \xrightarrow{h} V$ son aplicaciones, entonces $h(gf) = (hg)f$. En efecto, ambas tienen el mismo dominio S, el mismo rango T y, para cualquier $x \in S$,

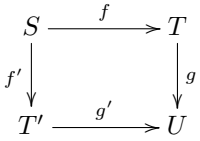
$$(h(gf))(x) = h((gf)(x)) = h(g(h(x))),$$
$$((hg)f)(x) = (hg)(f(x)) = h(g(f(x))),$$

por tanto que son la misma aplicación. Es usual escribir simplemente hgf para designarla.

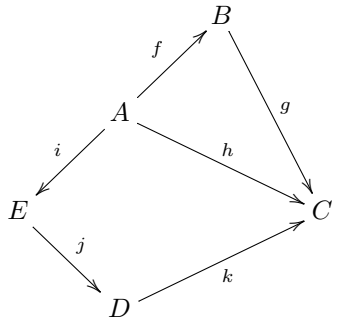
Si $S \xrightarrow{f} T \xrightarrow{g} U$ son aplicaciones componibles y $h : S \to U$ es una aplicación, es usual indicar la igualdad $h = gf$ diciendo que el triángulo



es conmutativo, o que $h \neq gf$, diciendo que el triángulo no es conmutativo. Análogamente, un rectángulo de aplicaciones



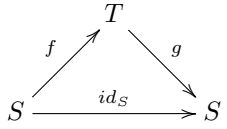
es conmutativo, si $gf = g'f'$. En general, la conmutatividad de un diagrama de aplicaciones, cuando tiene sentido, significa que las aplicaciones obtenidas por composición desde un vértice inicial hasta uno terminal según las diferentes rutas son la mismas. Por ejemplo, la conmutatividad del diagrama



significa que $gf = h = kji$.

Para cualquier conjunto S, se define la aplicación *identidad* en S, $id_S : S \to S$ (o 1_S, o 1 si S es claro por el contexto) como la aplicación tal que $id_S(x) = x$, para todo $x \in S$. Es la aplicación de S en si mismo cuyo grafo es la *diagonal* $\Delta = \{(x, x) \mid x \in S\}$. Si $f : S \to T$ es cualquier aplicación, uno verifica inmediatamente que $id_T f = f = f\, id_S$.

Lema 1.2.2. *Si $S \xrightarrow{f} T$ y $T \xrightarrow{g} S$ son dos aplicaciones tal que $gf = id_S$, es decir, tal que el triángulo*



conmuta, entonces f es inyectiva y g es sobreyectiva.

DEMOSTRACIÓN. Supongamos que $f(x) = f(y)$, para ciertos $x, y \in S$. Entonces $x = id_S(x) = gf(x) = gf(y) = id_S(y) = y$. Así que f es inyectiva. Dado cualquier $x \in S$, como $x = id_S(x) = gf(x) = g(f(x)$, es $x \in Im(g)$, luego g es sobreyectiva. □

Supongamos ahora que $S \xrightarrow{f} T$ tal que existe una otra $T \xrightarrow{g} S$ tal que $gf = id_S$ y $fg = id_T$. Entonces f es inyectiva y sobreyectiva, por el lema, y por tanto una biyección. Recíprocamente, si f es biyectiva, entonces podemos encontrar una aplicación $g : T \to S$ tal que $gf = id_S$ y $fg = id_T$: Para cada $y \in T$, sea $g(y) \in S$ el único elemento de S tal que $f(g(y)) = y$. Esto define una tal aplicación g, claramente verificando que $fg = id_T$. Además, para cualquier $x \in S$, como obviamente $x \mapsto f(x)$, es $g(f(x)) = x$, así que $gf = id_S$. Esto prueba que

Proposición 1.2.3. *Una aplicación $f : S \to T$ es biyectiva si y solo si existe una aplicación $g : Y \to X$ tal que $gf = id_S$ y $fg = id_T$.*

Para $f : S \to T$ una biyección, solo existe una aplicación $g : T \to S$ tal que $gf = id_S$ y $fg = id_T$: Si $g' : T \to S$ es otra con $g'f = id_S$ y $fg' = id_T$, entonces

$$g' = g'id_T = g'fg = id_Sg = g.$$

Esa única g es llamada la *inversa* de f y es denotada por f^{-1}. Si $f : S \to T$ es biyectiva, entonces su inversa $f^{-1} : T \to S$ es la única aplicación tal que $f^{-1}f = id_T$ y $ff^{-1} = id_T$. Observar que f^{-1} también es biyectiva y $(f^{-1})^{-1} = f$.

Como una primera aplicación del criterio de biyectividad anterior, podemos dar una demostración del hecho (bastante obvio) de que la composición de dos aplicaciones biyectivas es biyectiva: Sean $f : S \to T$ y $g : T \to U$ biyecciones, y consideremos su composición $gf : S \to U$. Entonces, tenemos sus inversas $g^{-1} : U \to T$ y $f^{-1} : T \to S$, y su compuesta $f^{-1}g^{-1} : U \to S$. Además

$$(f^{-1}g^{-1})(gf) = f^{-1}(g^{-1}(gf)) = f^{-1}((g^{-1}g)f) = f^{-1}(id_Tf) = f^{-1}f = id_S,$$
$$(gf)(f^{-1}g^{-1}) = g(f(f^{-1}g^{-1})) = g((ff^{-1})g^{-1}) = g(id_Tg^{-1}) = gg^{-1} = id_U.$$

Así que gf es biyectiva, con inversa

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

La siguiente observación para conjuntos finitos es útil en muchas ocasiones

Lema 1.2.4. *Sea S un conjunto finito. Las siguientes propiedades para $f : S \to S$ son equivalentes:*

1. *f es biyectiva.*
2. *f es inyectiva.*
3. *f es sobreyectiva.*

DEMOSTRACIÓN. Supongamos que $|S| = n$. Si f es inyectiva, entonces $|Im(f)| = n$, luego $Im(f) = S$ y f es sobreyectiva. Recíprocamente, si f no es inyectiva, entonces $|Im(f)| < n$, luego f no es sobreyectiva. □

1.2.1 Imágenes directas e inversas

Toda aplicación $f : S \to T$ determina otras

$$f_* : \mathcal{P}(S) \to \mathcal{P}(T), \quad f^* : \mathcal{P}(T) \to \mathcal{P}(S),$$

llamadas las aplicaciones *imagen* e *imagen inversas* por f, respectivamente, que están definidas, para cada $A \subseteq S$ y $X \subseteq T$, por

$$f_*(A) = \{f(a) \mid a \in A\}, \quad f^*(X) = \{a \in S \mid f(a) \in X\}.$$

Dejaremos como ejercicios las siguientes propiedades de las imágenes directas o inversas. Dada una aplicación $f : S \to T$, $A, B \subseteq S$ subconjuntos de S y $X, Y \subseteq T$ son subconjuntos de T.

1. Probar que $f^*(X \cup Y) = f^*(X) \cup f^*(Y)$ y $f_*(A \cup B) = f_*(A) \cup f_*(B)$.
2. Probar que $f^*(X \cap Y) = f^*(X) \cap f^*(Y)$ y $f_*(A \cap B) \subseteq f_*(A) \cap f_*(B)$.
3. Demostrar que si f es inyectiva, entonces $f_*(A \cap B) = f_*(A) \cap f_*(B)$.
4. Demostrar con el siguiente ejemplo que, en general, $f_*(A \cap B) \neq f_*(A) \cap f_*(B)$: Sea $f = |\ | : \mathbb{R} \to \mathbb{R}$ la aplicación "valor absoluto", $A = (0, 1)$ y $B = (-1, 0)$.
5. $f_*(f^*(X)) \subseteq X$, y se da la igualdad si f es sobreyectiva.
6. $A \subseteq f^*(f_*(A))$, y se da la igualdad si f es inyectiva.
7. Probar que, si f es una biyección entonces las aplicaciones $f_* : \mathcal{P}(S) \to \mathcal{P}(T)$ y $f^* : \mathcal{P}(T) \to \mathcal{P}(S)$ son biyectivas e inversas una de la otra.

Ejercicios

1. Sean $f : S \to T$ y $g : T \to U$ aplicaciones.
   (a) Probar que si ambas son inyectivas, entonces su composición $gf : S \to U$ es también inyectiva.
   (b) Probar que si ambas son sobreyectivas, entonces su composición $gf : S \to U$ es también es sobreyectiva.
   (c) Si su compuesta $gf : S \to U$ es inyectiva o sobreyectiva ¿qué podemos decir sobre f y g?
2. Sea $f : S \to T$ una aplicación.
   (a) Probar que f es inyectiva si y solo si tiene una *inversa por la izquierda*, es decir, existe una aplicación $g : T \to S$ tal que $gf = id_S$.
   (b) Dar un ejemplo de una aplicación inyectiva con dos diferentes inversas por la izquierda.
   (c) Probar que f es sobreyectiva si y solo si tiene una *inversa por la derecha*, es decir, existe una aplicación $g : T \to S$ tal que $fg = id_T$.
   (d) Dar un ejemplo de una aplicación sobreyectiva con dos diferentes inversas por la derecha.

3. En los siguientes ejercicios S y T son dos conjuntos arbitrarios, A, A' son subconjuntos de S y B, B' son subconjuntos de T.

   (a) i. Probar $A \times B$ es un subconjunto de $S \times T$.
   ii. Probar, con el siguiente ejemplo, que no todo subconjunto X de $S \times T$ es de la forma $X = A \times B$: $S = T = \{0, 1\}$, $X = \{(0, 0), (1, 1)\} \subseteq S \times T$.

   (b) Probar las siguientes igualdades:
   i. $c(A \times B) = c(A) \times T \cup S \times c(B)$.
   ii. $(A \cup A') \times B = (A \times B) \cup (A' \times B)$.
   iii. $(A \cap A') \times B = (A \times B) \cap (A' \times B)$.
   iv. $(A \cap A') \times (B \cap B') = (A \times B) \cap (A' \times B')$.
   v. $(A \cup A') \times (B \cup B') = (A \times B) \cup (A' \times B) \cup (A \times B') \cup (A' \times B')$.

4. Se consideran los subconjuntos de $\mathbb{R}$, $S = [-1, 1]$, $T = [-3, 4]$. Describir en dibujo los siguientes recintos de $\mathbb{R}^2$: $S \times T$, $T \times S$, $(S \times T) \cup (T \times S)$, $(S \times T) \cap (T \times S)$, $(S \times T) - (T \times S)$, $(T \times S) - (S \times T)$.

1.3 Relaciones de equivalencia. Conjuntos cocientes.

Definimos una *relación* (binaria) entre los elementos de un conjunto S (o, simplemente, en S) como un subconjunto $R \subseteq S \times S$.

Si $(a, b) \in R$, se dice que *a está relacionado con b por la relación R*, y se escribe aRb. Muchas relaciones tienen una o más de las siguientes propiedades:

- **Reflexiva**. $\forall a \in S$, aRa,.
- **Simétrica**. $\forall a, b \in S$, si aRb, entonces bRa.
- **Transitiva**. $\forall a, b, c \in S$, si aRb y bRc, entonces aRc.

Por ejemplo:

1. La relación "a es padre de b" referida al conjunto de los humanos, no tiene ninguna de estas propiedades.
2. La relación"a tiene los mismos parientes que b" tiene las tres.
3. La relación "a es antecesor de b" es transitiva.
4. La relación "a es hermano de b" es simétrica.

Una relación R en un conjunto S que es reflexiva, simétrica y transitiva es llamada una *relación de equivalencia* sobre S.

Una relación de equivalencia separa los elementos del conjunto S en *bloques* o *clases de equivalencia* donde se agrupan todos los elementos que se relacionan entre sí por la relación dada. Si $a \in S$ es cualquier elemento, definimos "*su clase de equivalencia*" o "*la clase de equivalencia que representa a*", denotada por $\bar{a}$ (o $[a]$), como el subconjunto de S

$$\bar{a} = \{x \in S \mid xRa\},$$

donde se reúnen todos los elementos equivalentes a a. Cada uno de estos subconjuntos es no vacío, pues por la reflexividad $a \in \bar{a}$, y se verifica que cualesquiera dos bloques $\bar{a}$, $\bar{b}$ bien son disjuntos o coinciden:

Proposición 1.3.1. *para cualesquiera $a, b \in S$, son equivalentes*

1. $\bar{a} \cap \bar{b} \neq \emptyset$.
2. aRb.
3. $\bar{a} = \bar{b}$.

Demostración. (1) $\Rightarrow$ (2): Supongamos que $\exists c \in \bar{a} \cap \bar{b}$. Como cRa y cRb, por la simetría, tenemos aRc y cRb, y entonces, por la transitividad, aRb.

(2) $\Rightarrow$ (3): Si $x \in \bar{a}$, entonces $xRa \wedge aRb \Rightarrow xRb \Rightarrow x \in \bar{b}$, así que $\bar{a} \subseteq \bar{b}$. Un argumento similar prueba que $\bar{b} \subseteq \bar{a}$ y por tanto $\bar{a} = \bar{b}$.

(3) $\Rightarrow$ (1) Es obvio. □

Resulta así que las diferentes clases de equivalencia proporcionan una descomposición S en subconjuntos no vacíos dos cualesquiera de ellos son disjuntos. Esto es lo que se llama una *partición* de S.

Por ejemplo, si R es la relación "a tiene los mismos parientes que b" entre los españoles, que es claramente de equivalencia, agrupa a los españoles en bloques conformados por las familias.

Si R es la relación entre los puntos del plano $\mathbb{R}^2$ estableciendo que pRq si p y q están a la misma distancia del origen, los bloques son las circunferencias $C_r = \bar{r}$ centradas en el origen y radio r, con $r \geq 0$.

Similarmente, si R es la relación "a da el mismo resto que b al dividirlo por 2" sobre el conjunto $\mathbb{N} = \{0, 1, \dots\}$ de los números naturales, esta relación parte el conjunto de naturales en dos subconjuntos disjuntos, de una parte el conjunto de los números pares, $\bar{[}0]$, y de otra el conjunto de los impares, $\bar{1}$.

Dada una relación de equivalencia R sobre un conjunto S, se define el *conjunto cociente de S por la relación R*, denotado S/R, como el conjunto cuyos elementos son los diferentes bloques o clases de equivalencia para tal relación:

$$S/R = \{\bar{a} \in \mathcal{P}(S) \mid a \in S\}.$$

En tal descripción, es muy importante tener claro que, aunque los elementos de S/R están parametrizados por los elementos a de S, tal parametrización no es unívoca pues tenemos que tener muy presente que

$$\bar{a} = \bar{b} \Leftrightarrow aRb.$$

Desde esa observación, puede pensarse en el conjunto cociente S/R como el *que se obtiene a considerar iguales (el mismo, identificados) todos los elementos de S que son equivalentes entre sí por la relación dada.*

Así, por ejemplo, para la relación R sobre $\mathbb{N}$ donde dos números son equivalentes si dan el mismo resto al dividirlos por 2, el conjunto cociente tiene exactamente dos elementos

$$S/R = \{\bar{0}, \bar{1}\},$$

puesto que para cualquier natural n, $\bar{n} = \bar{0}$ si n es par, y $\bar{n} = \bar{1}$ si n es impar.

Análogamente, Si R es la relación entre los puntos del plano $\mathbb{R}^2$ estableciendo que dos puntos p y q son equivalentes si están a la misma distancia del origen, el conjunto cociente

$$\mathbb{R}^2/R = \{C_r \mid r \in \mathbb{R}, r \geq 0\}$$

es el conjunto de las diferentes circunferencias centradas en el origen del plano $\mathbb{R}^2$ (¡sus elementos son circunferencias, no puntos!).

La proyección canónica. Dada una relación de equivalencia R en un conjunto S se tiene una aplicación que llamaremos la proyección canónica $p : S \to S/R$ y que lleva un elemento $x \in S$ en su clase de equivalencia, $p(x) = \bar{x}$. Esta aplicación es claramentee sobreyectiva.

La relación núcleo de una aplicación. Toda aplicación $f : S \to T$ da lugar a una relación de equivalencia R_f en su dominio S, definida por $xR_fy \Leftrightarrow f(x) = f(y), \forall x, y \in S$. Esta relación es llamada la relación núcleo de f.

Notación. A la relación úcleo de una aplicación f también la denotaremos como $\sim_f$.

Notemos que la relación de equivalencia asociada a la proyección canónica $p : S \to S/R$ es precisamente R, i.e. $R_p = R$.

La siguiente observación es muy útil para definir aplicaciones desde un conjunto cociente.

Proposición 1.3.2. *Sea R una relación de equivalencia sobre un conjunto S. Sea $f : S \to T$ una aplicación con la propiedad*

$$\forall a, b \in S, \text{ si } aRb \text{ entonces se verifica que } f(a) = f(b).$$

Entonces hay una aplicación $\bar{f} : S/R \to T$ *definida por la fórmula*

$$\bar{f}(\bar{a}) = f(a), \forall \bar{a} \in S/R.$$

Se verifica que $Im(\bar{f}) = Im(f)$*, por tanto que* $\bar{f}$ *es sobreyectiva si y solo si* f *lo es. Además* $\bar{f}$ *es inyectiva si y solo si se verifica que*

$$\forall a, b \in S, \text{ si } f(a) = f(b), \text{ entonces } aRb.$$

DEMOSTRACIÓN. Hemos de comprobar que la correspondencia $\bar{a} \mapsto f(a)$ define una aplicación de S/R en T. La primera condición de aplicación es clara, pues $\forall \bar{a} \in S/R$ tenemos que $(\bar{a}, f(a)) \in f$, esto es, todo elemento tiene asignada una imagen. Para ver la segunda, esto es que cada elemento tiene asignada una única imagen, supongamos que $(\bar{a}, f(a)), (\bar{b}, f(b)) \in S/R$, y que $\bar{a} = \bar{b}$. Entonces aRb y, por hipótesis, $f(a) = f(b)$. Luego, efectivamente, tenemos una aplicación bien definida.

La afirmación $Im(\bar{f}) = Im(f)$, y su consecuencia sobre la sobreyectividad, es inmediata. Para estudiar la inyectividad de $\bar{f}$, notemos que $\bar{f}(\bar{a}) = \bar{f}(\bar{b}) \Leftrightarrow f(a) = f(b)$. Par tanto, $\bar{f}$ será inyectiva si y solo si $f(a) = f(b) \Rightarrow \bar{a} = \bar{b}$ o, equivalentemente, $f(a) = f(b) \Rightarrow aRb$. □

La aplicación $\bar{f} : S/R \to T$ es llamada la *inducida por* f *en el cociente*. Esta asigna a cada clase de equivalencia el valor que f asigna a cualquiera de sus representantes lo que, lógicamente, explica la condición de que f sea constante sobre elementos relacionados.

EJEMPLO. Consideremos $[0, 1] \subseteq \mathbb{R}$, el intervalo cerrado de la recta real formado por los números t tales que $0 \leq t \leq 1$. Definamos en él la relación de equivalencia R por la que identificamos los puntos 0 y 1, y solo estos. Más precisamente, decimos que

$$tRu \Leftrightarrow \begin{cases} \text{si } t, u \in \{0, 1\} \\ t = u \text{ en otro caso} \end{cases}$$

De manera que el conjunto cociente $[0, 1]/R$ consiste del bloque $\bar{0} = \bar{1} = \{0, 1\}$ y de los bloques unitarios $\bar{t} = \{t\}$ con $0 < t < 1$.

Consideremos ahora la aplicación $f : [0, 1] \to C_1$, donde $C_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ es la circunferencia del plano real con radio 1 y centrada en el origen, definida por

$$f(t) = (cos(2\pi t), sen(2\pi t)), \quad 0 \leq t \leq 1.$$

Puesto que f es sobreyectiva y $f(t) = f(u) \Leftrightarrow tRu$, tenemos una biyección inducida

$$[0, 1]/R \cong C_1$$

que permite pensar a la circunferencia como el resultado de identificar los extremos del intervalo $[0, 1]$.

Como consecuencia inmediata de la Proposición 1.3.2 tenemos el siguiente

Teorema 1.3.3 (Descomposición canónica de una aplicación.)**.** *Dada una aplicación* $f : S \to T$ *existe un isomorfismo* $b : S/R_f \xrightarrow{\cong} Im(f)$ *que hace conmutar el siguiente diagrama:*

$$\begin{array}{ccc} S & \xrightarrow{\quad f \quad} & T \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ S/R_f & \xrightarrow[b]{\cong} & Im(f) \end{array}$$

donde p *es la proyección canónica e* i *es la inclusión.*

Demostración. Ya que, por definición $xR_f y \Leftrightarrow f(x) = f(y)$, la Proposición 1.3.2 nos permite definir $\bar{f} : S/R_f \to T$ como $\bar{f}(\bar{x}) = f(x)$ que además será inyectiva y cumple $fp(x) = f(x)$. Definimos entonces $b : S/R_f \to Im(f)$ como $b(\bar{x}) = \bar{f}(\bar{x}) = f(x)$ y tenemos el teorema. ■

Ejercicios

1. Sea $\mathbb{N} = \{0, 1, 2 \ldots, \}$ el conjunto de los números naturales, Sobre $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ definimos $(a, b) \sim (c, d)$ si $a + d = b + c$.

   (a) Verificar que $\sim$ es una relación de equivalencia.

   (b) Sea $f : \mathbb{N}^2 \to \mathbb{Z}$ la aplicación definida por $f(a, b) = a - b$. Verificar que f induce una biyección $\mathbb{N}^2/\sim \cong \mathbb{Z}$.

2. ¿Qué está mal en la siguiente demostración de que toda relación R sobre S que es simétrica y transitiva es reflexiva? Para $a, b \in S$, aRb, implica bRa (por simetría) y entonces (por transitividad) aRa.

3. Sea $f : S \to T$ una aplicación. Probar que, si f es sobreyectiva, induce una biyección $S/R_f \cong T$.

4. Sea $Y \subseteq X$ un subconjunto. Sea $f : \mathcal{P}(X) \to \mathcal{P}(Y)$ la aplicación tal que $f(A) = A \cap Y$, para cada $A \in \mathcal{P}(X)$.

   (a) Probar que f es una sobreyección.

   (b) Describir la relación R_f, núcleo de f.

   (c) Probar que f induce una biyección $\mathcal{P}(X)/R_f \cong \mathcal{P}(Y)$.

5. Sea R una relación de equivalencia sobre el conjunto S. La aplicación $p : S \to S/R$ definida por $p(a) = \bar{a}$ es llamada la *proyección canónica* de S sobre el cociente ¿Qué relación hay entre R y R_p?

6. Un subconjunto $P \subseteq \mathcal{P}(S)$, recordar, es llamado una *partición del conjunto* S si

   (a) $\forall A \in P,\ A \neq \emptyset$.

   (b) $\bigcup_{A \in P} A = S$.

   (c) Para cualesquiera $A, B \in P$, $A \neq B$, se verifica que $A \cap B = \emptyset$.

   Así, por ejemplo, el conjunto cociente S/R, para R una relación de equivalencia sobre S, es una partición.

   Sea P una partición de S. Definimos la aplicación $p : S \to P$ por $p(a) = A$ si $a \in A$. ¿Qué relación hay entre P y S/R_p?

Tema 2

Anillos conmutativos

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

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

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

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

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

Definición 2.0.1. *Un "anillo conmutativo" es un conjunto A en el que hay definidas dos operaciones, una denotada de forma aditiva y la otra de forma multiplicativa, tal que se cumplen las siguientes ocho propiedades:*

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

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

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

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

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

Podemos ya citar diversos ejemplos de referencia:

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

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

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

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

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

2.1 Los anillos $\mathbb{Z}_n$

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

Teorema 2.1.1. *Para cualesquiera enteros $a, b \in \mathbb{Z}$, con $b \neq 0$, existen dos únicos enteros $q, r \in \mathbb{Z}$, tales que*

1. $a = bq + r$,

2. $0 \leq r < |b|$.

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

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

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

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

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

Para cada natural $n \geq 2$, sea

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

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

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

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

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

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

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

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

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

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

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

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

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

Demostración. Claramente son conmutativas. Son asociativas:

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

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

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

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

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

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

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

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

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

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

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

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

2.2 Generalidades

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Supuesto cierto para un n,

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

□

La siguiente igualdad también es importante

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

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

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

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

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

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

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

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

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

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

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

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

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

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

y el "*anillo de racionales cuadráticos*"

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

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

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

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

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

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

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

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

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

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

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

2.4 Múltiplos y potencias naturales

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

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

1. $(m+n)a = ma + na$.
2. $n(a+b) = na + nb$.
3. $m(na) = (mn)a$.
4. $(ma)(nb) = (mn)(ab)$.
5. $a^n a^m = a^{n+m}$.
6. $(ab)^n = a^n b^n$.
7. $(a^m)^n = a^{mn}$.
8. $(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}$.
9. $(a+b)^2 = a^2 + 2ab + b^2$.
10. $(a+b)^3 = a^3 + 3a^2 b + 3ab^2 + b^3$.
11. $(a-b)(a+b) = a^2 - b^2$.

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

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

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

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

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

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

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

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

(8) Recordemos el significado de los términos binomiales

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

Y tengamos en cuenta la fórmula

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

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

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

Supuesta la validez para un n, entonces

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

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

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

2.5 Unidades. Cuerpos

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

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

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

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

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

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

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

EJEMPLOS.

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

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

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

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

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

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

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

Así, por ejemplo

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

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

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

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

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

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

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

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

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

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

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

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

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

Ejemplos.

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

2.6 Múltiplos negativos y potencias de exponente negativo

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

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

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

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

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

□

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

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

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

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

sin tampoco posible confusión por ubicación de paréntesis.

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

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

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

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

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

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

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

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

Finalmente,

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

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

(2) y (6):

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

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

(3) y (7):

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

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

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

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

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

(4):

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

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

□

2.7 Los anillos de polinomios $A[x]$

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

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

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

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

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

a las que nos referimos como polinomios*. Para un tal polinomio f, y cada natural $n \in \mathbb{N}$, el elemento $f(n) \in A$ se llama su "*coeficiente de grado n*".*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

y para $n \geq 1$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.8 Homomorfismos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Y existe, pues propuesto de esta forma, vemos que

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

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

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

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

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

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

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

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

Unos ejemplos,

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

Cada polinomio $f(x) \in A[x]$, define una aplicación $A \to A$, que asigna como imagen a cada elemento $a \in A$, el resultado de evaluar $f(x)$ en a, esto es $f(a)$. Se denota igual que el polinomio $f(x) : A \to A$ y se le llama la "*función polinómica definida por el polinomio* $f(x)$. Es importante no confundir la función polinómica con el polinomio, como muestra este ejemplo: Sean los polinomios de $\mathbb{Z}_2[x]$, $f(x) = 1 + x$ y $g(x) = 1 + x^2$. Sus correspondientes funciones polinómicas $f(x), g(x) : \mathbb{Z}_2 \to \mathbb{Z}_2$, funcionan así: $f(0) = 1 = g(0)$, $f(1) = 0 = g(1)$, esto es, son la misma! y los polinomios distintos.

Tema 3

Congruencias. Ideales y Cocientes

La construcción de cocientes aparece en la mayoría de los contextos algebraicos (conjuntos, anillos, grupos, monoides, etc.). Para hacer un cociente en estos contextos, necesitamos una congruencia, esto es, una relación de equivalencia que sea compatible con la estructura algebraica que estemos considerando. Esta compatibilidad permitirá trasladar la estructura al conjunto de clases de equivalencias, haciendo que la proyección canónica sea morfismo.

Definición 3.0.1. *Dado un anillo A, una congruencia (de anillos) en A es una relación de equivalencia $\equiv$ en A compatible con la estructura de anillo, lo que significa:*

- Compatible con la suma*:*

$$\left.\begin{array}{c} x \equiv y \\ z \equiv t \end{array}\right\} \Rightarrow x + z \equiv y + t.$$

- Compatible con el producto*:*

$$\left.\begin{array}{c} x \equiv y \\ z \equiv t \end{array}\right\} \Rightarrow xz \equiv yt.$$

- Compatible con los opuestos*:*

$$x \equiv y \Rightarrow -x \equiv -y.$$

Claramente la compatibilidad de los opuestos se deduce de la compatibilidad con el producto ya que

$$\left.\begin{array}{c} -1 \equiv -1 \\ x \equiv y \end{array}\right\} \Rightarrow -x \equiv -y.$$

Si $\equiv$ es una congruencia en A, podemos trasladar la estructura de anillo de A al conjunto de clases de equivalencia $A/\equiv$ de manera que la proyección canónica $pr : A \twoheadrightarrow A/\equiv$ sea un morfismo de anillos, definiendo suma, producto y opuestos en el cociente como sigue:

- $\bar{a} + \bar{b} := \overline{a + b}$,

- $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$,
- $-\bar{a} := \overline{-a}$.

Para todo $\bar{a}, \bar{b} \in A/\equiv$.

Dejamos como ejercicio comprobar que esta suma, producto y opuestos están bien definidos y que cumplen la axiomática de anillo.

El anillo $A/\equiv$ es el *anillo cociente de A por la congruencia $\equiv$.*

Definición 3.0.2. *El núcleo de una congruencia $\equiv$ en un anillo A se define como:*

$$Ker(\equiv) := \{a \in A;, a \equiv 0\}.$$

Destacamos las siguientes propiedades del núcleo de una congruencia:

- $0 \in Ker(\equiv)$
- Es cerrado para sumas: $a, b \in Ker(\equiv) \Rightarrow a + b \in Ker(\equiv)$.
- Es cerrado para opuestos $a \in Ker(\equiv) \Rightarrow -a \in Ker(\equiv)$.
- Es cerrado para múlltiplos $a \in Ker(\equiv), \forall x \in A \Rightarrow x \cdot a \in Ker(\equiv)$.

Estas propiedades dan lugar a la siguiente

Definición 3.0.3. *Un ideal de un anillo A es un subconjunto $I \subseteq A$ que tiene las siguientes propiedades:*

- $0 \in I$
- *Es cerrado para sumas:* $a, b \in I \Rightarrow a + b \in I$.
- *Es cerrado para opuestos* $a \in I \Rightarrow -a \in I$.
- *Es cerrado para múlltiplos* $a \in I, \forall b \in A \Rightarrow a \cdot b \in I$.

Es fácil de comprobar la siguiente

Proposición 3.0.4. *Un subconjunto no vacío $I \subseteq A$ es un ideal si, y sólo si, es cerrado para combinaciones lineales, esto es:*

$$\forall a, b \in I, \forall x, y \in A, xa + yb \in I.$$

Si I es un ideal de un anillo A escribiremos $I \leq A$.

Está claro que el núcleo de una congruencia es un ideal, veamos ahora que todo ideal determina una congruencia que lo tiene a el por núcleo.

Proposición 3.0.5. *Si $I \leq A$ es un ideal, entonces la relación definida por*

$$a \equiv_I b \Leftrightarrow a - b \in I,$$

es una congruencia con núcleo $ker(\equiv_I) = I$.

Demostración. Para ver que es congruencia tenemos que probar primero que es relación de equivalencia y después que es compatible con la estructura. Probamos solamente que es compatible con el producto, el resto de las propiedades las dejamos como ejercicio.

$$\left.\begin{array}{l} a \equiv b \Leftrightarrow a-b \in I \Rightarrow (a-b)c \in I \\ c \equiv d \Leftrightarrow c-d \in I \Rightarrow (c-d)b \in I \end{array}\right\} \overset{\text{sumando}}{\Rightarrow} (a-b)c+(c-d)b = ac-bd \in I \Rightarrow ac \equiv_I bd.$$

Si calculamos el núcleo

$$Ker(\equiv_I) = \{a \in A;\, a \equiv_I 0\} = \{a \in A;\, a-0 = a \in I\} = I.$$

■

Notemos ahora que dada una congruencia $\equiv$ en A, la relación $\equiv_{Ker(\equiv)}$ es la propia $\equiv$. De manera que tenemos:

Teorema 3.0.6. *Dar una congruencia en un anillo A es equivalente a dar un ideal de A.*

Observación 3.0.1. Dado un idea $I \leq A$ si $a \equiv_I b$ diremos que a es congruente con b módulo I y a veces también lo denotaremos $a \equiv b \mod I$.

Observación 3.0.2. Después del Teorema 3.0.6 tenemos que toda congruencia en A es de la forma $\equiv_I$ para $I \leq A$ un ideal. Al conjunto cociente $A/\equiv_I$ lo denotaremos simplemente por A/I y sus elementos serán clases de equivalencia módulo I. Veamos ahora como es la clase de equivalencia de un elemento $a \in A$ módulo I.

$$\bar{a} = \{x \in A;\, x \equiv_I a\} = \{x \in A;\, x-a \in I\} = a+I.$$

Donde $a+I$ es el conjunto de los elementos de A que se escriben de la forma $a+y$ con $y \in I$. Así,

$$A/I = \{a+I;\, a \in A\}$$

y la suma, el producto y los opuestos están definidos como:

- $(a+I)+(b+I) := (a+b)+I$,
- $(a+I)\cdot(b+I) := (a\cdot b)+I$,
- $-(a+I) := (-a)+I$.

Además la proyección canónica $pr : A \twoheadrightarrow A/I$ lleva un elemento $a \in A$ en $pr(a) = a+I \in A/I$.

Ejemplo 3.0.1. Todo anillo A tiene dos ideales *improòios*, el ideal cero $0 = \{0\} \leq A$ y el ideal *total* $A \leq A$.

Ejemplo 3.0.2. Si A es un anillo y $a \in A$ es un elemento, los múltiplos de a, que denotamos aA es un ideal de A. Está claro que los ideales impropios son los múltiplos de cero y de uno respectivamente. $0 = 0A$ y $A = 1A$.

Definición 3.0.7. *Un ideal $I \leq A$ se dirá principal si existe un elemento $a \in A$ tal que $I = aA$.*

El Teorema 2.1.1 de Euclides nos permite demostrar:

Teorema 3.0.8. *En el anillo $\mathbb{Z}$ todo ideal es principal.*

Demostración. El ideal trivial es claramente principal, supongamos entonces un ideal no trivial $I \leq \mathbb{Z}$, denotemos $I^+ = \{a \in I;\ 0 < a\} \subseteq \mathbb{N}$.

Puesto que si $a \in I$ entonces $-1 \cdot a = -a \in I$ e I es no trivail, tenemos que $I^+ \neq \emptyset$ y por tanto podemos tomar $a = min(I^+)$. Puesto que $a \in I^+ \subseteq I$ tenemos que $aA \subseteq I$. Recíprocamente, sea $b \in I$ un elemento cualquiera, ya que $a \neq 0$, podemos dividir b por a y tenemos que existen $q, r \in \mathbb{Z}$ tales que $b = aq + r$ y $0 \leq r < |a| = a$. Veamos que $r = 0$. Si no fuese cero, tendríamos que $r = b - aq \in I^+$ y $r < a$, que contradice que $a = min(I^+)$. Por tanto $r = 0$ y $b = aq \in aA$. Así $I \subseteq aA$ y tenemos la igualdad. ■

Observación 3.0.3. Por el Teorema 3.0.8 todo ideal de $\mathbb{Z}$ será de la forma $n\mathbb{Z}$ y sus elementos serán los múltiplos de $n \in Z$. Notemos que $n\mathbb{Z} = -n\mathbb{Z}$ y por tanto todo ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ con $n \geq 0$. Además en lugar de escribir $a \equiv_{n\mathbb{Z}} b$ o $a \equiv b \mod n\mathbb{Z}$ escribiremos $a \equiv_n b$ o $a \equiv b \mod n$ y diremos que a es congruente con b módulo n, para $a, b, n \in \mathbb{Z}$ y $n \geq 0$.

3.1 El primer teorema de Isomorfía

Dado un morfismo de anillos $f : A \to B$ su núcleo está definido como

$$\ker f = \{a \in A;\ f(a) = 0\}.$$

Está claro que $0 \in \ker f$ y que $\ker f$ es cerrado para combinaciones lineales y por tanto $\ker f$ es un ideal de A, $\ker f \leq A$.

Observación 3.1.1. Si $\equiv$ es una congruencia en A, entonces

$$\ker \equiv = \ker pr$$

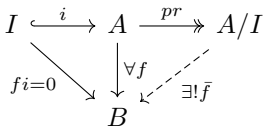
con $pr :: A \twoheadrightarrow A/\equiv$ la proyección canónica.

En particular, si $I \leq A$ es un ideal, $\ker \equiv_I = I$.

La proyección canónica $pr : A \twoheadrightarrow A/I$ tienen la siguiente propiedad universal:

Proposición 3.1.1 (Propiedad universal de la proyección canónica)**.**

Dado un ideal $I \leq A$ dar un morfismo $\bar{f} : A/I \to B$ es equivalente a dar un morfismo $f : A \to B$ tal que $f^*(I) = 0$. Sintetizamos esta propiedad mediante el siguiente diagrama:



$$\bar{f}(a + I) = f(a)$$

Demostración. La demostración de esta proposición consiste en ver que dado un morfismo $f : A \to B$ podemos definir $\bar{f} : A/I \to B$ por $\bar{f}(a + I) := f(a), \forall a \in A$, si, y sólo si, $f(y) = 0, \forall y \in I$. Pero, utilizando la proposición 1.3.2 podemos definir la aplicación $\bar{f}$ si, y sólo si, $\forall a, b \in A$ se tiene que $a \equiv_I b$ implique $f(a) = f(b)$. Basta entonces considerar:

$$a \equiv_I b \Leftrightarrow a - b \in I \Rightarrow f(a - b) = 0 \Rightarrow f(a) = f(b).$$

Así si todos los elementos de I van a 0 por f podemos definir $\bar{f}$ que claramente es un morfismo. El recíproco es claro. ■

Teorema 3.1.2 (Primer teorema de Isomorfía)**.**

Dado un morfimso de anillos $f : A \to B$ existe un isomorfismo de anillos $b : A/\ker f \xrightarrow{I} m(f)$ que hace comnmutar el diagrama

$$\begin{array}{ccc} A & \xrightarrow{pr} & A/\ker f \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle b\cong} \\ B & \longleftarrow & Im(f) \end{array} \tag{3.1}$$

Demostración. El morfismo b está definido como $b(a+\ker f) := f(a)$. Utilizando la propiedad universal de la proyección claramente b está bien definido. Es rutinario probar que es morfismo, que es una biyección y que hace conmutar el diagrama 3.1. ■

Ejemplo 3.1.1. Tomemos $n \geq 2$ un entero y consideremos la aplicación $R : \mathbb{Z} \to \mathbb{Z}_n$ que a cada entero $a \in \mathbb{Z}$ le hace corresponder el resto de dividir a entre n. Esta aplicación es n morfismo de anillos y claramente es sobreyectivo ya que si $0 < a$ entonces $R(a) = a$. Además el resto de dividir a por n es cero si, y sólo si, a es un múltipo de n, pro tanto $\ker R = n\mathbb{Z}$. El primer teorema de isomoría nos asegura que se tiene un isomorfismo

$$b : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}_n;\ a + n\mathbb{Z} \mapsto R(A).$$

3.2 Operaciones con ideales

Sea A un anillo y sean $I, J \leq A$ dos ideales. Entonces:

- La intersección $I \cap J$ es un ideal.
- En general la unión $I \cup J$ no lo es.
- La suma $I + J = \{a + b;\ a \in I, b \in J\}$ es un ideal. Además este es el menor ideal que contiene a I y a J.
- El producto, definido como

$$IJ = \{\sum_{i=1}^{r} a_i b_i;\ a_i \in I, b_i \in J\},$$

  es un ideal, que además está contenido en la intersección $IJ \subseteq I \cap J$.

Dejamos como ejercicio probar las afirmaciones anteriores.

Observación 3.2.1. El producto de dos elementos ab con $a \in I$ y $b \in J$ es un elemento de IJ, pero la suma de dos de estos productos $a_1b_1 + a_2b_2, a_i \in I, b_j \in J, i = 1, 2$, no tiene porqué ser un producto de este tipo, es decir no tiene porqué existir $a_3 \in I$ y $b_3 \in J$ tal que $a_1b_1 + a_2b_2 = a_3b_3$. A esto se debe que el producto de dos ideales se defina del modo que se ha hecho.

Sin embargo si hay un caso en el que el producto de dos ideales tiene una forma sencilla, este es cuando los ideales son principales, en cuyo caso es fácil comprobar:

$$aAbA = (ab)A.$$

Tema 4

Divisibilidad en Dominios de Integridad

Ecuaciones sencillas, como $ax = b$, con $a \neq 0$, no son sencillas de resolver en el contexto de un anillo conmutativo arbitrario (a diferencia de las del tipo $a + x = b$, que siempre tiene solución única: $x = b - a$). Si estamos en un cuerpo K (como $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$, etc.), tal ecuación siempre tiene solución $x = ba^{-1}$, y esta es única. Pero, en general, puede no tener solución (por ejemplo, $2x = 3$ en $\mathbb{Z}$), y puede tener más de una (por ejemplo, $2x = 2$ en $\mathbb{Z}_6$, tiene dos: $x = 1$, $x = 4$). En lo que sigue, nos centraremos en anillos conmutativos donde las ecuaciones $ax = b$, con $a \neq 0$, caso de tener solución, esta es única. Estos anillos son los "*Dominios de integridad*", que presentamos a continuación.

4.1 Dominios de Integridad

Un anillo conmutativo no trivial ($1 \neq 0$) es un Dominio de Integridad (DI, para acortar) si en él se verifica la "*propiedad cancelativa*":

$$\text{Si } a \neq 0, \text{ entonces } ax = ay \Rightarrow x = y.$$

En adelante, los anillos serán serán supuestos no triviales.

Proposición 4.1.1. *Un anillo conmutativo A es un DI si y solo si el producto de elementos no nulos es no nulo, esto es, si*

$$a \neq 0 \wedge b \neq 0 \Rightarrow ab \neq 0,$$

o, equivalentemente,

$$ab = 0 \Rightarrow a = 0 \vee b = 0.$$

Demostración.

$\Rightarrow$) Si $ab = 0$, tendríamos que $ab = a0$. Si $a \neq 0$ tendría que ser $b = 0$, al estar en un DI.

$\Leftarrow$) Supongamos $ax = ay$, con $a \neq 0$. Entonces $a(x - y) = 0$ y será $x - y = 0$, es decir que $x = y$.

■

Proposición 4.1.2.

1. *Cualquier subanillo de un DI es un DI.*
2. *Todo cuerpo es un DI.*

Demostración.

1. Si la propiedad cancelativa se verifica para todos los elementos no nulos de un anillo, obviamente se verifica para los de un subanillo suyo.
2. Si A es cuerpo, todo elemeto no nulo es unidad. Si $a \neq 0$ y $ax = ay$, multiplicando por a^{-1}, obtenemos que $a^{-1}ax = a^{-1}ay$, de donde $x = y$.

■

Ejemplos.

1. $\mathbb{Z}$, que es un subanillo de $\mathbb{Q}$ o de $\mathbb{R}$, es un DI. También los anillos $\mathbb{Z}[\sqrt{n}]$, que son todos subanillos de $\mathbb{C}$, son DI.
2. El anillo $\mathbb{Z}_4$ no es un DI, pues $2 \cdot 2 = 0$.
3. Si A es un DI, en anillo de polinomios $A[x]$ es in DI. Para ver esto, introduzcamos una terminología:

   - Para un polinomio no nulo $f(x) = \sum_{m\geq 0} a_m x^m$, decimos que su "*grado*" es r, si $a_r \neq 0$ y $a_n = 0$ para todo $n > r$.

   Si $g(x) = \sum_{m\geq 0} b_m x^m$ es otro no nulo de grado, digamos s, entonces los coeficientes del producto en grados $n > r + s$, $\sum_{i+j=n} a_i b_j$ son todos nulos, pues $i + j > r + s$ obliga a que bien $i > r$ o bien $j > s$, o sea que $a_i = 0$ o $b_j = 0$ en todos los sumandos. Por otra parte, el coeficiente de grado $r + s$ del producto es $\sum_{i+j=r+s} a_i b_j = a_r b_s$, pues si $i < r$ entonces ha de ser $j > s$ (para que sumen $r + s$) y entonces $b_j = 0$.

   Conclusión:

   - En general
   $$gr(fg) \leq gr(f) + gr(g).$$
   Pero puede darse que $gr(fg) < gr(f)gr(g)$: En $\mathbb{Z}_6[x]$, sea $f(x) = 3 + 2x$ y $g(x) = 3x$. Entonces $fg = x$ y $gr(fg) = 1 < gr(f) + gr(g) = 1 + 1 = 2$.

   Ahora, si el anillo A es un DI, entonces el coeficiente en grado $r + s$ de fg es $a_r b_s \neq 0$, pues $a_r \neq 0$ y $b_s \neq 0$. Luego $fg \neq 0$, y concluimos que $A[x]$ es un DI. Además, se da la igualdad
   $$gr(fg) = gr(f) + gr(g)$$
   para todos los polinomios no nulos $f, g \in A[x]$, siempre que A sea un DI.

Una observación interesante está dada en la siguiente

Proposición 4.1.3. *Si A es un DI finito, entonces es un cuerpo.*

Demostración. Sea $a \in A$, $a \neq 0$. La aplicación $f : A \to A$ definida por $f(x) = ax$ es inyectiva, y por tanto biyectiva. Luego existe un $x \in A$ tal que $ax = 1$. Esto es, $a \in U(A)$. ■

Hemos visto que todo subanillo de un cuerpo es un DI. La relación entre dominios de integridad y cuerpos es mucho más estrecha: todo DI es subanillo de un cuerpo, como vemos a continuación.

4.2 El cuerpo de fracciones de un DI

Sea A un DI. En el conjunto

$$A \times (A\backslash\{0\}) = \{(a,s) \mid a,s \in A, s \neq 0\}$$

establecemos la relación

$$(a,s) \sim (b,t) \Leftrightarrow at = bs.$$

Claramente es reflexiva y simétrica. Para ver que es transitiva, supongamos $(a,s) \sim (b,t) \sim (c,u)$, de manera que $at = bs \wedge bu = ct$. Entonces, $atu = bsu = cts$. Como $t \neq 0$, simplificando en la igualdad $tau = tcs$, y obtenemos que $au = cs$, así que $(a,s) \sim (c,u)$.

Consideremos el conjunto cociente $A \times (A\backslash\{0\})/\sim$ y denotaremos $\frac{a}{s}$ a la clase de equivalencia del par (a,s) (esto es, $\frac{a}{s} = \overline{(a,s)}$). Llamaremos a este elemento "*fracción de numerador a y denominador b*". Entonces,

$$\frac{a}{s} = \frac{b}{t} \Leftrightarrow at = bs.$$

Al conjunto cociente $A \times (A\backslash\{0\})/\sim$ le donotaremos por $\mathbb{Q}(A)$. Así que

$$\mathbb{Q}(A) = \Big\{\frac{a}{s} \mid a,s \in A, a \neq 0\Big\}.$$

Definimos ahora en $\mathbb{Q}(A)$ una suma y un producto por

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}, \quad \frac{a_1}{s_1}\frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2},$$

que están bien definidas:
Si $\frac{a_1}{s_1} = \frac{b_1}{t_1}$ y $\frac{a_2}{s_2} = \frac{b_2}{t_2}$, entonces

$$\frac{a_1 s_2 + a_2 s_1}{s_1 s_2} = \frac{b_1 t_2 + b_2 t_1}{t_1 t_2} \text{ y } \frac{a_1 a_2}{s_1 s_2} = \frac{b_1 b_2}{t_1 t_2},$$

pues

$$(a_1 s_2 + a_2 s_1)t_1 t_2 = a_1 s_2 t_1 t_2 + a_2 s_1 t_1 t_2 = b_1 s_1 s_2 + b_2 s_1 s_2 t_1 = (b_1 t_2 + b_2 t_1) s_1 s_2 \text{ y}$$
$$a_1 a_2 t_1 t_2 = b_1 s_1 b_2 s_2 = b_1 b_2 s_1 s_2.$$

Así, $\mathbb{Q}(A)$ resulta un anillo conmutativo, que además es un cuerpo:

- Su "cero" es $\frac{0}{1}$ $(=\frac{0}{s}$, para cualquier $s \neq 0)$.
- El opuesto de una fracción $\frac{a}{s}$ es $-\frac{a}{s} = \frac{-a}{s} = \frac{a}{-s}$.
- Su "uno" es $\frac{1}{1}$ $(=\frac{s}{s}$, para cualquier $s \neq 0)$.
- Además, si $\frac{a}{s} \neq \frac{0}{1}$, entonces $a \neq 0$ y $\frac{s}{a} \in \mathbb{Q}(A)$ y se verifica que $\frac{a}{s}\frac{s}{a} = \frac{as}{as} = \frac{1}{1}$. Luego $(\frac{a}{s})^{-1} = \frac{s}{a}$.

Al cuerpo $\mathbb{Q}(A)$ se le llama "*el cuerpo de fracciones de* A".

Por ejemplo, es claro que $\mathbb{Q}(\mathbb{Z}) = \mathbb{Q}$ el cuerpo de los números racionales.

En $\mathbb{Q}(A)$, una fracción de denominador 1, $\frac{a}{1}$ está univocamente determinada por el numerador ($\frac{a}{1} = \frac{b}{1} \Leftrightarrow a = b$), y la representaremos simplemente por el numerador. Esto es, ponemos $a = \frac{a}{1}$. De esta forma $A \subseteq \mathbb{Q}(A)$ como un subanillo. Pero notemos que los elementos a de A pueden ser representados en $\mathbb{Q}(A)$ por las diferentes fracciones equivalentes a $\frac{a}{1}$. Así, por ejemplo, en $\mathbb{Q} = \mathbb{Q}(\mathbb{Z})$, $-2 = \frac{-2}{1} = \frac{6}{-3}$.

Observación 4.2.1. Si K es un cuerpo, entonces $K = \mathbb{Q}(K)$.

En efecto, para cualquier $\frac{a}{s} \in \mathbb{Q}(K)$, como $s \neq 0$, $s^{-1} \in K$ y, entonces, $as^{-1} \in K$. Pero $as^{-1} = \frac{as^{-1}}{1} = \frac{a}{s}$, luego $\frac{a}{s} \in K$.

Esto nos permite utilizar legítimamente la notación de fracciones en cualquier cuerpo: $as^{-1} = \frac{a}{s}$. Por ejemplo, en $\mathbb{R}$, tenemos que

$$\frac{1}{2} = 2^{-1}, \ \ \frac{3}{2} = 3 \cdot 2^{-1}, \ \ (\sqrt{2})^{-1} = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}, \ \ \frac{\sqrt{2}}{\sqrt{3}} = \sqrt{2}(\sqrt{3})^{-1}, \ \textit{etc.}$$

Por ejemplo, es fácil comprobar que todo elemento no nulo de $\mathbb{Z}_5$ es una unidad, por ejemplo $3^{-1} = 2$ así podremos escribir

$$2 \cdot 3^{-1} = \frac{2}{3} = 2 \cdot 4.$$

Y esto permite a su vez la siguiente regla operativa para las fracciones en cualquier cuerpo (en $\mathbb{Q}(A)$, en particular.)

$$\frac{\frac{a}{s}}{\frac{b}{t}} = \frac{a}{s}\left(\frac{b}{t}\right)^{-1} = \frac{a}{s}\frac{t}{b} = \frac{at}{bs}.$$

Observación 4.2.2. Si $A \subseteq B$, entonces $\mathbb{Q}(A) \subseteq \mathbb{Q}(B)$.

Observación 4.2.3. Si $A \subseteq K$, donde K es un cuerpo, entonces $\mathbb{Q}(A) \subseteq \mathbb{Q}(K) = K$. Así que, "$\mathbb{Q}(A)$ *es el menor cuerpo que contiene a* A".

Observación 4.2.4. *El cuerpo de fracciones de* $\mathbb{Z}[\sqrt{n}]$ *es* $\mathbb{Q}[\sqrt{n}]$. En efecto, sabemos que $\mathbb{Q}[\sqrt{n}]$ es un cuerpo y $\mathbb{Z}[\sqrt{n}] \subseteq \mathbb{Q}[\sqrt{n}]$. Por tanto, el cuerpo de fracciones de $\mathbb{Z}[\sqrt{n}]$ está contenido en $\mathbb{Q}[\sqrt{n}]$. Por otra parte, cualquier cuerpo que contenga a $\mathbb{Z}[\sqrt{n}]$ contiene a $\mathbb{Q}[\sqrt{n}]$, pues al contener a $\mathbb{Z}$ también contiene a $\mathbb{Q} = \mathbb{Q}(\mathbb{Z})$, y entonces a todo número de la forma $a+b\sqrt{n}$ con $a, b \in \mathbb{Q}$, esto es, contiene a $\mathbb{Q}[\sqrt{n}]$. En particular, el cuerpo de fracciones de $\mathbb{Z}[\sqrt{n}]$ contiene a $\mathbb{Q}[\sqrt{n}]$.

4.3 Divisibilidad

En lo que sigue A es un DI. El estudio de la ecuación $ax = b$, conduce de forma natural a estudiar la relación de "*divisibilidad*" entre elementos del anillo, que se establece como sigue.

Definición 4.3.1. *Dados* $a, b \in A$*, decimos que "*a divide a b*", situación que representamos por "*$a|b$*", o que "*a es un divisor de b*" o también que "*b es un múltiplo de a*", si existe un* $c \in A$ *tal que* $ac = b$.

Esto es, $a|b$ si la ecuación $ax = b$ tiene solución, la cual, si $a \neq 0$, será necesariamente única, pues A es un DI.

El caso $a = 0$, se discute de forma trivial:

$$0|b \Leftrightarrow b = 0.$$

Esto es, 0 solo es divisor del cero, o, en otras palabras, 0 es el único múltiplo del 0.

Notemos ahora que cuando $a \neq 0$, podemos expresar la relación $a|b$ en términos de $\mathbb{Q}(A)$:

$$a|b \Leftrightarrow \frac{b}{a} \in A.$$

En efecto, si $a|b$, existirá un $c \in A$ tal que $ac = b$, en cuyo caso $\frac{b}{a} = \frac{ac}{a} = \frac{c}{1} = c \in A$. Y recíprocamente, si $\frac{b}{a} \in A$, será $\frac{b}{a} = c = \frac{c}{1}$ para algún $c \in A$, en cuyo caso $b = ac$ y, por tanto, $a|b$.

Las siguientes son propiedades elementales de la relación de divisibilidad.

1. (Reflexiva) $a|a$.
2. (Transitiva) $a|b \wedge b|c \Rightarrow a|c$.
3. Si $a|b$ y $a|c$, entonces $a|(bx + cy)$, para todo $x, y \in A$.
4. Si $c \neq 0$, entonces $a|b \Leftrightarrow ac|ab$.

Observación 4.3.1. Todos los elementos del anillo dividen a 0, esto es, $a|0$ para todo $a \in A$ (pues $a0 = 0$).

Observación 4.3.2. Los *divisores de 1* son precisamente los elementos invertibles del anillo, es decir los elementos del conjunto $U(A)$ de unidades de A.

Ejemplos.

1. $U(\mathbb{Z}) = \{1, -1\}$.
2. $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.
3. $U(A[x] = U(A)$. En efecto, es claro que $U(A) \subseteq U(A[x])$. Si $f(x) = \sum_m a_m x^m \in U(A[x])$, existirá $g(x) = \sum_m b_m x^m \in A[x]$ tal que $f(x)g(x) = 1$. Pero entonces $gr(f(x)) + gr(g(x)) = 0$, así que $gr(f(x)) = 0 = gr(g(x))$. Esto es, $f(x) = a_0 \in A$, $g(x) = b_0 \in A$ y $a_0 b_0 = 1$. En particular $f(x) = a_0 \in U(A)$.
4. $U(\mathbb{Z}[x]) = \{1, -1\}$, $U(\mathbb{Q}[x]) = \mathbb{Q} - \{0\}$, $U(\mathbb{Z}_3[x]) = \{1, 2\}$, etc.

Observación 4.3.3. Las unidades del anillo son divisores de todos los elementos del anillo: Si $u \in U(A)$, entonces para todo elemento a, se tiene que $a = a1 = (au^{-1})u$, así que $u|a$. También ocurre que si multiplicamos cualquier elemento a por una unidad u el resultado ua es un divisor de a, pues $a = (ua)u^{-1}$. Así que, para cualquier elemento a, los elementos del conjunto

$$\{u, ua \mid u \in U(A)\}$$

son siempre divisores de a, les llamamos los "*divisores triviales*" de a. Por ejemplo, en $\mathbb{Z}$, los divisores triviales del 2 son $\{1, -1, 2, -2\}$. En el anillo $\mathbb{Z}[i]$ de los enteros de Gauss, los divisores triviales de $1 + i$ son

$$\{1, -1, i, -i, 1 + i, -1 - i, -1 + i, 1 - i\}.$$

Observación 4.3.4. Para cada elemento a, los divisores triviales de la forma ua, con $u \in U(A)$, se llaman "*asociados*" de a. Observar que, dada cualquier unidad $u \in U(A)$, tenemos que $u^{-1} \in U(A)$ y $b = ua \Leftrightarrow a = u^{-1}b$. Por tanto un elemento b es asociado de un a si y solo si este a es asociado de b. Hablamos simplemente de que "*a y b son asociados*".

Estos se pueden caracterizar como sigue.

Proposición 4.3.2. *Para cualesquiera $a, b \in A\backslash\{0\}$, son equivalentes*

1. *a y b son asociados.*
2. *$a/b \ \wedge \ b/a$.*

Demostración. Es claro que si a y b son asociados, cada uno es divisor del otro. Recíprocamente, supongamos que a y b se dividen mutuamente. Digamos que $b = ua$ y que $a = vb$. Entonces $a = uva$ y, como $\neq 0$, es $uv = 1$. Luego $u, v \in U(A)$ y a y b son asociados. ■

Definición 4.3.3. *Un elemento $a \in A$, se dice que es "*irreducible*" si no es cero ni unidad y sus únicos divisores son los triviales, esto es, las unidades y sus asociados.*

Proposición 4.3.4. *Un elemento $a \in A$, no nulo ni unidad, es irreducible si y solo si se verifica que, dada cualquier factorización suya en producto de dos elementos entonces uno de los factores es una unidad (y entonces el otro un asociado); esto es:*

$$a \text{ es irreducible } \Leftrightarrow a = bc, \text{ entonces } b \in U(A) \text{ o } c \in U(A).$$

Demostración.

$\Rightarrow$) Supongamos que $a = bc$ y que $b, c \notin U(A)$. Como b y c son divisores triviales, ambos serán asociados de a. Digamos que $b = ua$ y que $c = va$, con $u, v \in U(A)$. Entonces $a = uava = uva^2$. Como $a \neq 0$, será $1 = (uv)a$, y concluimos que a es una unidad, lo que supone una contradicción.

$\Leftarrow$) Supongamos que $b|a$. Será $a = bc$ para un cierto $c \in A$. Entonces $b \in U(A)$ o $c \in U(A)$. Si $b \in U(A)$, b es un divisor trivial. Si $b \notin U(A)$, será $c \in U(A)$, y por tanto b un asociado de a.

■

Ejercicios.

1. Argumenta si los siguientes anillos son, o no, Dominios de Integridad:

$$\mathbb{Z}_8, \ \ \mathbb{Z}[\sqrt{2}], \ \ \mathbb{Z}_3, \ \ \mathbb{Z} \times \mathbb{Z}, \ \ \mathbb{Z}_6[x], \ \ \mathbb{Z}[i], \ \ \mathbb{Z}_5[x].$$

2. Es el anillo definido por el conjunto $\mathbb{Z} \times \mathbb{Z}$ con las operaciones

$$(a, a') + (b, b') = (a + b, a' + b') \text{ y } (a, a')(b, b') = (ab, ab' + a'b),$$

un Dominio de Integridad?

3. ¿Es el anillo definido por el conjunto $\mathbb{Z}$ de los números enteros con las operaciones $a \oplus b = a + b - 1$ y $a \otimes b = a + b - ab$ un Dominio de Integridad? integridad?

4. Se define el cuerpo $\mathbb{Q}(x)$ como el cuerpo de fracciones del anillo $\mathbb{Z}[x]$, esto es $\mathbb{Q}(x) = \mathbb{Q}(\mathbb{Z}[x])$. Describe como son sus elementos y sus operaciones.

5. Demuestra que $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$ tienen el mismo cuerpo de fracciones. Esto es,

$$\mathbb{Q}(\mathbb{Q}[x]) = \mathbb{Q}(x).$$

6. Sea $A = \{\frac{m}{2^k} \in \mathbb{Q} \mid m \in \mathbb{Z} \text{ y } k \geq 0\}$. Argumentar que

   (a) A es subanillo de $\mathbb{Q}$.

   (b) $\mathbb{Z} \subsetneq A$.

   (c) El cuerpo de fracciones de A es el mismo que el de $\mathbb{Z}$, o sea $\mathbb{Q}$.

7. Argumentar la veracidad o falsedad de las siguientes porposiciones referidas a elementos de un Dominio de Integridad

   (a) $a \,|\, b \wedge a \nmid b \Rightarrow b \nmid b + c$.

   (b) $a \nmid b \wedge a \nmid c \Rightarrow a \nmid b + c$.

8. ¿Es la relación "ser divisor de" una relación de orden entre los elementos de un DI?

9. En un Dominio de Integridad A establecemos la relación $\sim$ diciendo que $a \sim b$ si a es asociado con b.

   (a) Probar que $\sim$ es una relación de quivalencia en A.

   (b) Sea $A/\!\sim = \{\bar{a} \mid a \in A\}$, el correspondiente conjunto cociente. Establecemos entre sus elementos la relación por la cual $\bar{a} \leq \bar{b}$ si a es un divisor de b en al anillo A ¿Está bien definida esa relación en $A/\!\sim$? ¿Es una relación de orden?.

Tema 5

Dominios Euclídeos

Hay un tipo de dominios de integridad, los llamados "*Dominios Euclídeos*" (DE, por acortar), donde se dispone de una herramienta eficaz para saber si un elemento a divide a otro b; esto es, si la ecuación $ax = b$ tiene solución y, en su caso, resolverla.

Definición 5.0.1. *Sea A un DI. Se dice que A es un DE, si es especificada una aplicación $\rho : A - \{0\} \to \mathbb{N} = \{0, 1, ...\}$, que llamaremos la "*función euclídea*", tal que*

1. *$\rho(ab) \geq \rho(a)$, $\forall\, a, b \in A$, $a, b \neq 0$.*

2. *$\forall\, a, b \in A$, con $b \neq 0$, $\exists\, q, r \in A$ tal que $a = bq + r$, donde $r = 0$ o $\rho(r) < \rho(b)$.*

Nos referimos a "q" y a "r" como un cociente y un resto de dividir a entre b (¡no exigimos su unicidad!).

Proposición 5.0.2. *Sea A es un DE, para $a, b \in A - \{0\}$ son equivalentes:*

1. *$b|a$.*

2. *Todo resto de dividir a entre b es 0.*

3. *0 es un resto de dividir a entre b.*

Demostración.
(1) $\Rightarrow$ (2):
Si $b|a$ existe $c \in A$ tal que $a = bc$. Supongamos que $a = bq + r$ con $r = 0$ o $\rho(r) < \rho(b)$. Hemos de ver que necesariamente $r = 0$. En efecto, en otro caso, tenemos $r = a - bq = bc - bq = b(c - q)$ y, en particular, $c - q \neq 0$. pero entonces $\rho(r) = \rho(b(c - q)) \geq \rho(b)$, lo que supone una contradicción a que $\rho(r) < \rho(b)$.
Las implicaciones (2) $\Rightarrow$ (3) y(3) $\Rightarrow$ (1) son inmediatas. ■

Observación 5.0.1. Claramente $\mathbb{Z}$, por el Teorema de Euclides, es un DE con función euclídea el valor absoluto $|\ | : \mathbb{Z} \to \mathbb{N}$ (que en este caso está definida incluso para el 0). Vemos ahora que los anillos de polinomios $K[x]$, con K un cuerpo, son también DE.

Teorema 5.0.3. *Sea K un cuerpo. Para cualesquiera polinomios $f(x), g(x) \in K[x]$, con $g(x) \neq 0$, existen dos únicos polinomios $q(x), r(x) \in K[x]$ tales que $f(x) = g(x)q(x) + r(x)$ donde $r(x) = 0$ o $gr(r(x)) < gr(g(x))$.*

Demostración.

Probemos primero la unicidad: Supongamos $f(x) = g(x)q(x)+r(x)$ donde $r(x) = 0$ o $gr(r(x)) < gr(g(x))$ y $f(x) = g(x)q'(x) + r'(x)$, donde $r'(x) = 0$ o $gr(r'(x)) < gr(g(x))$. Y Supongamos que fuera $r(x) \neq r'(x)$. Entonces $r(x) - r'(x) \neq 0$ y claramente $gr(r(x) - r'(x)) < gr(g(x))$. Además, como $r(x) - r'(x) = g(x)(q'(x) - q(x)) \neq 0$, también es $q'(x) - q'(x) \neq 0$, y tendríamos también que $gr(r(x)-r'(x)) = gr(g(x))+gr(q'(x)-q(x)) \geq gr(g(x))$, lo que supone una contradicción. Luego $r(x) = r'(x)$ y, entonces, también $q(x) = q'(x)$.

Veamos ahora la existencia: Es claro que podemos reducirnos al caso en que $f(x) \neq 0$ y $gr(f(x)) \geq gr(g(x))$ (en otro caso $q(x) = 0$ y $r(x) = f(x)$ serían los cocientes y el resto). Supongamos que $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{m} b_i x^i$, con $a_n \neq 0$ y $b_m \neq 0$, de manera que $n = gr(f(x)) \geq m = gr(g(x))$. Y haremos la demostración por inducción en n, el grado de $f(x)$.

Si $n = 0$, como $m \leq n$, será también $m = 0$, así que $f(x) = a_0 \in K$ y $g(x) = b_0 \in K$. La igualdad $a_0 = b_0(b_0^{-1}a_0) + 0$ nos dice que el cociente es $b_0^{-1}a_0$ y el resto 0.

Supuesto $n > 0$, y realizada la hipótesis de inducción, construyamos el polinomio

$$\begin{aligned} f_1(x) &= f(x) - a_n b_m^{-1} x^{n-m} g(x) \\ &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 - (a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \cdots + a_n b_m^{-1} b_0 x^{n-m}) \end{aligned}$$

que claramente resulta de grado menor que n. Por hipótesis de inducción, existen polinomios $q_1(x)$ y $r(x)$ con $f_1(x) = g(x)q_1(x) + r(x)$, donde bien es $r(x) = 0$ o $gr(r_1(x)) < gr(g(x))$. Pero entonces tenemos la igualdad

$$\begin{aligned} f(x) &= f_1(x) + a_n b_m^{-1} x^{n-m} g(x) = g(x)q_1(x) + r(x) + a_n b_m^{-1} x^{n-m} g(x) \\ &= g(x)(q_1(x) + a_n b_m^{-1} x^{n-m}) + r(x) = g(x)q(x) + r(x), \end{aligned}$$

y concluimos que el cociente es $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ y el resto $r(x)$. ■

Tenemos entonces que

Teorema 5.0.4. *el anillo $K[x]$ es un DE con función euclídea la función grado.*

No siempre hay unicidad de cocientes y restos. En los siguentes ejemplos de DE, los anillos de enteros cuadráticos, $\mathbb{Z}[\sqrt{-2}] = \mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$ y $\mathbb{Z}[\sqrt{3}]$, tal cosa no ocurre.

Teorema 5.0.5. *Para $n = -2, -1, 2, 3$ los anillos $\mathbb{Z}[\sqrt{n}]$ son DE, con función euclídea definida por $\rho(\alpha) = |N(\alpha)|$.*

Demostración.

Recordar que, para cualquier $a + b\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$, su norma es

$$N(a + b\sqrt{n}) = (a + b\sqrt{n})(a - b\sqrt{n}) = a^2 - nb^2,$$

que un racional, pero entero si a y b lo son.

Sean $\alpha = a + b\sqrt{n}, \beta = c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, dos enteros cuadráticos no nulos. La primera condición de DE es fácil de probar:

$$|N(\alpha\beta)| = |N(\alpha)|\,|N(\beta)| \geq |N(\alpha)| \quad \text{(pues } |N(\beta)| \geq 1)$$

Para la segunda condición, supongamos que $|\mathbb{N}(\alpha)| \geq |\mathbb{N}(\beta)|$. Hemos de probar que existen $q = q_1 + q_2\sqrt{n}$ y $r = r_1 + r_2\sqrt{n}$ en $\mathbb{Z}[\sqrt{n}]$ tal que $\alpha = \beta q + r$, donde bien es $r = 0$ o $|N(r)| < |N(\beta)|$ en otro caso. Para ello, procedemos como sigue.

Recordar que el cuerpo de fracciones de $\mathbb{Z}[\sqrt{n}]$ es $\mathbb{Q}[\sqrt{n}]$. Consideramos entonces la fracción $\frac{\alpha}{\beta}$ y la expresamos como un elemento de $\mathbb{Q}[\sqrt{n}]$, mediante el procedimiento de "*racionalizar*":

$$\begin{aligned}\frac{\alpha}{\beta} &= \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = \frac{1}{N(\beta)}(a+b\sqrt{n})(c-d\sqrt{n}) = \frac{1}{N(\beta)}\Big((ac-bdn)+(cb-ad)\sqrt{n}\Big)\\ &= \frac{ac-bdn}{N(\beta)} + \frac{cb-ad}{N(\beta)}\sqrt{n} = a_1 + a_2\sqrt{n},\end{aligned}$$

donde, claramente, $a_1, a_2 \in \mathbb{Q}$. Seleccionamos enteros $q_1, q_2 \in \mathbb{Z}$ con la condición de que $|a_1 - q_1| \leq \frac{1}{2}$, $|a_2 - q_2| \leq \frac{1}{2}$. Llamamos entonces $q = q_1 + q_2\sqrt{n}$ y $r = \alpha - \beta q$. Claramente $q, r \in \mathbb{Z}[\sqrt{n}]$ y $\alpha = \beta q + r$. Bastará que probemos que, si $r \neq 0$, entonces $|N(r)| < |N(\beta)|$. Para ello, trabajando en el cuerpo de fracciones $\mathbb{Q}[\sqrt{n}]$, notemos que

$$\begin{aligned}|N(r)| = |N(\alpha - \beta q)| &= \Big|N\Big(\beta\Big(\frac{\alpha}{\beta} - q\Big)\Big)\Big| = |N(\beta)|\,\Big|N\Big(\frac{\alpha}{\beta} - q\Big)\Big|\\ &= |N(\beta)|\,\big|N\big((a_1-q_1)+(a_2-q_2)\sqrt{n}\big)\big|\\ &= |N(\beta)|\,\big|(a_1-q_1)^2 - n(a_2-q_2)^2\big| = |N(\beta)|\,|A|.\end{aligned}$$

donde hemos denotado $A = (a_1 - q_1)^2 - n(a_2 - q_2)^2$. Y será suficiente probar que $|A| < 1$. Vemos esto en cada caso $n = -1, -2, 2, 3$:

- Si $n = -1$, $A = (a_1 - q_1)^2 + (a_2 - q_2)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$.
- Si $n = -2$, $A = (a_1 - q_1)^2 + 2(a_2 - q_2)^2 \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1$.
- Si $n = 2$, $A = (a_1 - q_1)^2 - 2(a_2 - q_2)^2$, donde $0 \leq (a_1 - q_1)^2 \leq \frac{1}{4}$ y $0 \leq 2(a_2 - q_2)^2 \leq \frac{1}{2}$. Entonces $-\frac{1}{2} \leq A \leq \frac{1}{4}$ y $|A| \leq \frac{1}{2} < 1$.
- Si $n = 3$, $A = (a_1 - q_1)^2 - 3(a_2 - q_2)^2$, donde $0 \leq (a_1 - q_1)^2 \leq \frac{1}{4}$ y $0 \leq 3(a_2 - q_2)^2 \leq \frac{3}{4}$. Entonces $-\frac{3}{4} \leq A \leq \frac{1}{4}$ y $|A| \leq \frac{3}{4} < 1$.

■

Ejemplo de no unicidad en los cocientes y restos.

En el anillo $\mathbb{Z}[i]$, se verifica que $11 + 7i = (2i)(3 - 5i) + (1 + i)$, donde $N(1 + i) = 2 < 4 = N(2i)$. Luego $3 - 5i$ y $1 + i$ son un cociente y un resto de dividir $11 + 7i$ entre $2i$. Pero también $11 + 7i = (2i)(4 - 6i) + (-1 - i)$, donde $N(-1 - i) = 2 < 4 = N(2i)$. Luego $4 - 6i$ y $-1 - i$ son también un cociente y un resto de dividir $11 + 7i$ entre $2i$.

Ejercicios.

1. Con un recipiente de 67 litros ¿podré rellenar con precisión un depósito de 1207 litros? (No. La ecuación $67x = 1207$ no tiene solución, pues $1207 = 67 \cdot 18 + 1$ y 67 no divide a 1208).
2. ¿Es $f(x) = 2x^4 - 3x^3 + 6x + 10$ divisor de $g(x) = 6x^6 - 9x^5 + 2x^4 + 15x^3 + 30x^2 + 6x + 10$ en el anillo $\mathbb{Q}[x]$? (Si, $g(x) = f(x)(3x^2 + 1)$.
3. ¿Es $f(x) = 2x^4 - 3x^2 + 6x + 10$ divisor de $g(x) = 6x^6 - 9x^5 + 2x^4 + 15x^3 + 30x^2 + 8x + 10$ en el anillo $\mathbb{Q}[x]$? (No, $g(x) = f(x)(3x^2 + 1) + 2x$.)
4. ¿Es $f(x) = 1 + 3x^2$ divisor de $g(x) = 2 + 3x + 4x^3 + 2x^4$ en el anillo $\mathbb{Z}_5[x]$? (Si, $g(x) = f(x)(2 + 3x + 4x^2)$.

5. Resolver la ecuación $(7+2\sqrt{2})x = 4+7\sqrt{2}$.

6. Resolver la ecuación $3i\,x = 11+7i$ en $\mathbb{Z}[i]$.

7. ¿Podremos rellenar con precisión un depósito de 538.833 litros usando un recipiente de 371? En caso afirmativo ¿Cuantas veces usaremos el recipiente?

8. Determinar, si existe, un polinomio $f(x) \in \mathbb{Q}[x]$ tal que
$$\Big(\frac{3}{5}x^3+\frac{1}{2}x+\frac{2}{3}\Big)f(x) = \frac{9}{20}x^5+\frac{147}{40}x^3+\frac{1}{2}x^2+\frac{11}{4}x+\frac{11}{3}.$$

9. Calcular el cociente y el resto de dividir, en el anillo $\mathbb{Q}[x]$, el polinomio $\frac{9}{20}x^5+\frac{147}{40}x^3+\frac{1}{2}x^2+\frac{17}{4}x+\frac{17}{3}$ entre el polinomio $\frac{3}{5}x^3+\frac{1}{2}x+\frac{2}{3}$.

10. Determinar, si existe, un polinomio $f(x) \in \mathbb{Z}_3[x]$ tal que
$$(2x^2+x+2)f(x) = 2x^7+x^6+2x^4+2.$$

11. En el anillo $\mathbb{Z}[i]$, calcular cociente y resto de dividir $1+15i$ entre $3+5i$.

12. ¿Es $2+5\sqrt{3}$ un divisor de $39-9\sqrt{3}$ en el anillo $\mathbb{Z}[\sqrt{3}]$?

5.1 Máximo común divisor

Nos vamos a continuación abordar las ecuaciones de la forma $ax+by=c$ en el contexto de Dominios Euclídeos. Estas son ecuaciones clásicamente estudiadas en el contexto del anillo $\mathbb{Z}$ de los números enteros, donde surgen de forma muy natural. Por ejemplo, con recipientes de 6 y 15 litros, ¿podré rellenar con precisión un depósito de 39 litros?. Si x es el número de veces que uso el recipiente de 6 e y el de 15, será por que $6x+9y=39$, y así trasformamos el problema en una ecuación diofántica (Se puede hacer, usando 4 veces el de 6 y una vez el de 15). Para estudiar y resolver tales ecuaciones será fundamental el concepto de máximo común divisor, que presentamos a continuación.

En lo que sigue A es un DI.

Definición 5.1.1. *Dados dos elementos $a,b \in A$, decimos que un elemento $d \in A$ es un máximo común divisor (mcd, para acortar) de a y b, y escribiremos $d = mcd(a,b)$ o bien $d=(a,b)$ (si en el contexto no hay confusión), si tiene las siguientes dos propiedades:*

1. *$d|a \wedge d|b$.*
2. *Si $c|a \wedge c|b$, entonces $c|d$.*

Ambas condiciones en conjunto significan que los divisores de d son exactamente los divisores comunes a a y b.

El mcd de dos elementos en un DI, si existe, no es único. Si $d=(a,b)$, claramente lo es también cualquier asociado con d (pues tienen los mismos divisores). Y recíprocamente, si también $d'=(a,b)$ entonces d y d' tienen los mismos divisores, y en particular, se dividen mutuamente, luego d y d' son asociados. Así que d es único salvo asociados. Con esta salvedad, hablaremos de que "*d es el mcd de a y b*", abusando del artículo determinado.

Definición 5.1.2. *Decimos que a y b son "* primos relativos *" o "* primos entre sí *", si $(a,b)=1$.*

Notemos que el concepto de mcd se extiende sin dificultad a un conjunto finito de elementos $a_1, ..., a_n \in A$: d es un mcd de ellos, cosa que escribiremos poniendo $d = mcd(a_1, ..., a_n)$ o bien $d = (a_1, ..., a_n)$, si:

1. $d|a_i \ \forall i = 1, ...n$ y,
2. si un $c|a_i \ \forall i = 1, ...n$, entonces $c|d$.

Las siguientes son propiedades generales, que se satisfacen siempre que existan los máximos comunes divisores que se ven involucrados en los enunciados (las igualdades hay que leerlas "salvo asociados"):

1. $(a, b) = (b, a)$.
2. Si a y a' son asociados, entonces $(a, b) = (a', b)$.
3. $(a, b) = a \Leftrightarrow a|b$. En particular $(a, 0) = a$, $(a, 1) = 1$.
4. $((a, b), c) = (a, b, c) = (a, (b, c))$.
5. $(ac, bc) = (a, b)c$.

   Podemos limitarnos al caso en que $a, b, c \neq 0$. Sea $d = (a, b)$ y $(ac, bc) = e$. Como $dc|ac \wedge dc|bc$, será $dc|e$. Supongamos que $e = dcu$. Por otra parte, como $dcu|ac$ y $dcu|bc$, resulta que $du|a$ y $du|b$, de donde $du|d$. Por tanto será $d = duv$, lo que implica que $1 = uv$ ($d \neq 0$ pues $a \neq 0$ es un múltiplo suyo). Así que $u \in U(A)$ y e es asociado con dc, luego dc es también el mcd de ac y bc, pues e lo es. En conclusión $(a, b)c = (ac, bc)$.
6. Si $d = (a, b)$, y $a = da'$ y $b = db'$ entonces $(a', b') = 1$.

   Como $d(a'b') = (da', db') = (a, b) = d = d \cdot 1$, basta simplificar por d.
7. Si $a|bc$ y $(a, b) = 1$, entonces $a|c$.

   Pongamos $bc = ax$. Entonces $c = c1 = c(a, b) = (ac, bc) = (ac, ax) = a(c, x)$.
8. Si $(a, b) = 1$, entonces $a|c \wedge b|c \Rightarrow ab|c$.

   Pongamos $c = bx$. Como $a|bx$ y $(a, b) = 1$, será $a|x$. Pongamos $x = ay$. Entonces $c = aby$.
9. $(a, b) = 1 \wedge (a, c) = 1 \Leftrightarrow (a, bc) = 1$.

   $\Rightarrow$]: $c = c1 = c(a, b) = (ac, bc)$. Entonces

   $$1 = (a, c) = (a, (ac, bc)) = ((a, ac), bc) = (a, bc).$$

   $\Leftarrow$]: $1 = (a, bc) = ((a, ac), bc) = (a, (ac, bc)) = (a, (a, b)c)$. Como (a, b) es un divisor común a a y a $(a, b)c$, será (a, b) un divisor de uno, o sea una unidad. Luego $(a, b) = 1$. De la primera igualdad, $1 = (a, (a, b)c)$, se sigue que también $(a, c) = 1$.
10. $(a, b) = (a - qb, b)$.

    Si $c|a \wedge c|b$, entonces $c|a - qb \wedge a|b$. Si $c|a - qb \wedge c|b$, entonces $c|a - qb + qb = b \wedge c|b$. Luego los divisores comunes a a y b son los mismos que los divisores comunes a $a - qb$ y b. Tendrán por tanto el mismo mcd.

11. Si p es irreducible, entonces $(p,a) = \begin{cases} p & \text{si } p|a, \\ 1 & \text{en otro caso.} \end{cases}$

Observación 5.1.1. No siempre existe el mcd de dos cualesquiera elementos en un DI.

EJEMPLO. *En* $\mathbb{Z}[\sqrt{-5}]$ *no existe* $(2+2\sqrt{-5},6)$.

En efecto. Observamos primero que, en este anillo, 3 es irreducible. Supongamos que por el contrario que $3 = \alpha\beta$, donde ni α ni β son unidades. O sea que $N(\alpha) \neq 1 \neq N(\beta)$. Entonces, la igualdad $N(3) = 9 = N(\alpha)N(\beta)$, obligaría a que $N(\alpha) = 3 = N(\beta)$. Pero, para cualesquiera $a, b \in \mathbb{Z}$,

$$N(a + b\sqrt{-5}) = 3 \Leftrightarrow a^2 + 5b^2 = 3$$

y no existen números enteros a y b de forma que se verifique tal igualdad.

Observamos ahora que 3 no divide a $1+\sqrt{-5}$, pues $N(3) = 9$ no es un divisor en $\mathbb{Z}$ de $N(1+\sqrt{-5}) = 1 + 25 = 26$. Entonces $(3, 1+\sqrt{-5}) = 1$.

Supongamos ahora que existiera $(2+2\sqrt{-5},6)$. Tendía que ser entonces

$$(2+2\sqrt{-5},6) = 2(1+\sqrt{-5},3) = 2 \cdot 1 = 2.$$

Pero ocurre que $1+\sqrt{-5} \,|\, 2+2\sqrt{-5}$ (pues $2+2\sqrt{-5} = 2(1+\sqrt{-5})$) y $1+\sqrt{-5}\,|6$ (pues $6 = N(1+\sqrt{-5}) = (1+\sqrt{-5})(1-\sqrt{-5})$), y tendría que ocurrir que $1+\sqrt{-5}\,|2$. Pero esto es falso, $N(1+\sqrt{-5}) = 6$, $N(2) = 4$ y 6 no es un divisor de 4 en $\mathbb{Z}$.

Hay dominios de integridad, sin embargo, donde la existencia de mcd está garantizada. Es el caso de los DE. Para probarlo, comenzamos con la siguiente

Proposición 5.1.3. *En un DE, todo ideal es principal.*

Demostración. Sea A un DE, e I un ideal suyo. Siempre $0 \in I$ (pues si $x \in I$, entonces $0 = 0x \in I$). Si $I = \{0\}$, entonces $I = 0A$ y es principal generado por el cero.

Supuesto I con elementos no nulos, consideremos

$$R = \{\rho(b) \mid b \in I, b \neq 0\} \subseteq \mathbb{N}.$$

Este conjunto no vacío de naturales tendrá un mínimo, digamos dado por $\rho(m)$. Como $m \in I$ e I es cerrado para múltiplos, será $mA \subseteq I$. Veamos que $I \subseteq mA$. En otro caso, tendríamos un $a \in I$ tal que m no divide a a. Pongamos $a = bm + r$ donde $r = 0$ o $\rho(r) < \rho(m)$. Claramente, no puede ser $r = 0$, o sea que $r \neq 0$ y $\rho(r) < \rho(m)$. Pero esto no es posible ya que $r = a + (-b)m \in I$, luego $\rho(r) \in R$, y $\rho(m)$ es mínimo en R. ■

Teorema 5.1.4. *Si A es un DE, existe el mcd de cualesquiera dos elementos. Además, si $d = (a,b)$, siempre es posible encontrar dos elementos $u, v \in A$ tales que*

$$d = au + bv,$$

*que son llamados "*coeficientes de Bezout de a y b*".*

Demostración. Dados $a, b \in A$, consideremos

$$I = aA + bA = \{ax + by \mid x, y \in A\}.$$

Es un ideal de A y será principal. Supongamos que $I = dA$. Como $a, b \in I = dA$, será $d|a$ y $d|b$. Además, como $d \in I$, será $d = au + bv$ para ciertos $u, v \in A$. Por otro lado, si $c|a$ y $c|b$ entonces $c|au + bv = d$. Luego $d = (a,b)$ y u, v son coeficientes de Bezout. ■

En un DE tenemos un algoritmo para el cálculo de mcd y coeficientes de Bezout. Es conocido como el ALGORITMO EXTENDIDO DE EUCLIDES, y es como sigue:

Si uno de los elementos involucrados es nulo, la cuestión es fácil:

$$(a, 0) = a = 1 \cdot a + 0 \cdot 0.$$

Supongamos entonces que $a, b \neq 0$, y podemos suponer entonces que $\rho(a) \geq \rho(b)$ (recordar que $(a, b) = (b, a)$. El algoritmo consiste en construir, recursivamente, una sucesión de elementos del anillo $r_1, r_2, \ldots, r_n$ partiendo de $r_1 = a$ y $r_2 = b$, por el siguiente procedimiento:

Si $r_i \neq 0$ entonces r_{i+1} es un resto de dividir r_{i-1} entre r_i.

Así, r_3 es el resto de dividir $r_1 = a$ entre $r_2 = b$. Si $r_3 \neq 0$, entonces r_4 es el resto de dividir r_2 entre r_3, etc.

Puesto que para todo i, $\rho(r_{i+1}) < \rho(r_i)$, la sucesión de números naturales $\rho(r_2) = \rho(b)$, $\rho(r_3)$, ..., $\rho(r_i)$, ... es estrictamente decreciente, y esta no puede continuar indefinidamente; esto es, habrá un $n \geq 1$ tal que $r_{n+1} = 0$. Pues bien, aseguramos que entonces

$$r_n = (a, b),$$

esto es el último de los restos no nulos obtenidos en tal sucesión es el mcd de a y b. En efecto, probamos por inducción que, para todo $i = 1, 2, ..., n$, se verifica que $(a, b) = (r_i, r_{i+1})$. Para $i = 1$, esto es obvio, pues $r_1 = a$ y $r_2 = b$. Supongamos que $i > 1$ y que $(a, b) = (r_{i-1}, r_i)$. Si q_i es el cociente de dividir r_{i-1} entre r_i, será $r_{i+1} = r_{i-1} - r_i q_i$. Entonces

$$(a, b) = (r_{i-1}, r_i) = (r_i, r_{i-1} - r_i q_i) = (r_i, r_{i+1}).$$

Finalmente, $(a, b) = (r_{n-1}, r_n) = r_n$, ya que $r_n | r_{n-1}$ al ser $r_{n+1} = 0$.

Vamos ahora que podemos encontrar, para todo $i = 1, ..., n$, elementos $u_i, v_i \in A$ tal que $r_i = au_i + bv_i$, por la reglas recursivas

- $u_1 = 1$, $v_1 = 0$.
- $u_2 = 0$, $v_1 = 1$.

y para $i \geq 2$,

- $u_{i+1} = u_{i-1} - q_i u_i$, $u_{i+1} = u_{i-1} - q_i u_i$.

En efecto, para $i = 1$ e $i = 2$, es obvio que $r_i = au_i + bu_i$. Supongamos esto cierto hasta un $i \geq 2$. Entonces

$$r_{i+1} = r_{i-1} - q_i r_i = au_{i-1} + bv_{i-1} - q_i(au_i + bv_i) = a(u_{i-1} - q_i u_i) + a(v_{i-1} - q_i v_i) = au_{i+1} + bv_{i+1}.$$

En última instancia, tenemos que $r_n = (a, b) = au_n + bv_n$, y habremos encontrado unos coeficientes de Bezout: $u = u_n$, $v = v_n$.

Vamos a sintetizar los datos anteriores en una tabla que nos permitirá no solo calcular el mcd de dos elementos, sino también los coeficientes de Bezout

	a	1	0
	b	0	1
q_2	r_3	$u_3 = 1 - 0 \cdot q_2$	$v_3 = 0 - q_2 \cdot 1$
...	...	...	...
q_{i-2}	r_{i-1}	u_{i-1}	v_{i-1}
q_{i-1}	r_i	u_i	v_i
q_i	r_{i+1}	$u_{i+1} = u_{i-1} - u_i \cdot q_i$	$v_{i+1} = v_{i-1} - q_i \cdot v_i$
...	...	...	...

EJEMPLOS.

1. En $\mathbb{Z}$, calcular $(80, 30)$ y unos correspondientes coeficientes de Bezout.
   La tabla

$$\begin{array}{cc|cc} & 80 & 1 & 0 \\ & 30 & 0 & 1 \\ 2 & 20 & 1 & -2 \\ 2 & 10 & -1 & 3 \\ & 0 & & \end{array}$$

   nos indica que $(80, 20) = 10$ y $10 = (-1) \cdot 80 + 3 \cdot 30$.

2. En el anillo $\mathbb{Z}[i]$, calcular $(11+7i, 3+7i)$ y unos correspondientes coeficientes de Bezout.
   La tabla

$$\begin{array}{cc|cc} & 11+7i & 1 & 0 \\ & 3+7i & 0 & 1 \\ 1-i & 1+3i & 1 & -1+i \\ -2 & 1+i & -2 & 3-2i \\ & 0 & & \end{array}$$

   nos indica que $(11+7i, 3+7i) = 1+i$ y $1+i = (-2)(11+7i) + (3-2i)(3+7i)$.

3. En el anillo $\mathbb{Z}_2[x]$, calcular $(x^3+x^2+x+1, x^4+x^3+x+1)$ y unos correspondientes coeficientes de Bezout.
   La tabla

$$\begin{array}{cc|cc} & x^4+x^3+x+1 & 1 & 0 \\ & x^3+x^2+x+1 & 0 & 1 \\ x & x^2+1 & 1 & x \\ & 0 & & \end{array}$$

   nos indica que $(x^3+x^2+x+1, x^4+x^3+x+1) = x^2+1$ y $x^2+1 = 1 \cdot (x^4+x^3+x+1) + x \cdot (x^3+x^2+x+1)$.

4. En el anillo $\mathbb{R}[x]$, calcular $(x^5+x^4+2x^3+2x^2+x+1, x^4+x^3+2x^2+x+1)$ y unos correspondientes coeficientes de Bezout.
   La tabla

$$\begin{array}{cc|cc} & x^5+x^4+2x^3+2x^2+x+1 & 1 & 0 \\ & x^4+x^3+2x^2+x+1 & 0 & 1 \\ x & x^2+1 & 1 & -x \\ & 0 & & \end{array}$$

   nos indica que $(x^5+x^4+2x^3+2x^2+x+1, x^4+x^3+2x^2+x+1) = x^2+1$ y

   $x^2+1 = 1 \cdot (x^5+x^4+2x^3+2x^2+x+1) + (-x) \cdot (x^4+x^3+2x^2+x+1)$.

5.2 Ecuaciones diofánticas

En lo que sigue A es un DE.

Teorema 5.2.1. *Sea la ecuación $ax+by=c$, donde $a, b \neq 0$, y sea $d = (a, b)$.*

1. *La ecuación tiene solución si y solo si $d|c$.*

2. *Si (x_0, y_0) es una solución particular, entonces la solución general consiste de todos los pares (x, y), donde*

$$\begin{cases} x = x_0 + k\frac{b}{d}, \\ y = y_0 - k\frac{a}{d} \end{cases}$$

Demostración. Al mismo tiempo que lo demostramos, "aprenderemos" a resolver tales ecuaciones.

Pongamos $a = da'$ y $b = db'$. Si la ecuación tiene soluciones, digamos que (x, y) es una de ellas, entonces, como $d|a$ y $d|b$, será $d|ax + by = c$. Así que, si d no divide a c, la ecuación no tiene solución.

Supongamos ahora que $d|c$. Pongamos $c = dc'$. La ecuación se escribe entonces como $da'x + db'y = dc'$, o sea $d(a'x + b'y) = dc'$, que claramente es equivalente a la ecuación

$$a'x + b'y = c'$$

donde $(a', b') = 1$. Nos referimos a esta como la reducida de la original. La novedad es que los coeficientes son ahora primos relativos. Podemos entonces encontrar $u, v \in A$, tal que $1 = a'u + b'v$. Entonces $c' = a'(c'u) + b'(c'v)$, vemos así que la ecuación tiene solución, y que (x_0, y_0), con $x_0 = c'u$ e $y_0 = c'v$, es una solución particular.

Para determinar todas las soluciones, notemos que, para cualquier $k \in K$, $(x_0 + kb', y_0 - ka')$ es también una solución:

$$a'(x_0 + kb') + b'(y_0 - ka') = a'x_0 + ka'b' + b'y_0 - ka'b' = a'x_0 + b'y_0 = c'.$$

Y no hay más soluciones que esas: Si (x, y) fuese cualquier otra, de las igualdades $a'x + b'y = c' = a'x_0 + b'y_0$, se deduce que $a'(x - x_0) = b'(y_0 - y)$. Pero entonces $b'|a'(x - x_0)$ y, ya que $(a', b') = 1$, será $b'|(x - x_0)$. Así que, para algún $k \in A$, $x - x_0 = kb'$. Análogamente, $a'|b'(y_0 - y)$ y, ya que $(a', b') = 1$, será $a'|(y_0 - y)$, de donde concluimos que $y_0 - y = ha'$, para un cierto $h \in A$. Pero, sustituyendo en la igualdad $a'(x - x_0) = b'(y_0 - y)$, vemos que $a'b'k = a'b'h$, de donde concluimos que $h = k$. Así que

$$x = x_0 + kb' = x_0 + k\frac{b}{d},\ x = y_0 - ka' = y_0 - k\frac{a}{d}.$$

■

Ejercicios.

1. "Cuarenta y seis náufragos cansados arribaron a una bella isla. Allí encontraron ciento veintiséis montones de cocos, de no más de cincuenta cada uno, y catorce cocos sueltos, y se los repartieron equitativamente . . ." (cuento del año 850 a.c.). ¿Cuántos cocos había en cada montón?

2. Disponemos de 15 euros para comprar 40 sellos de correos, de 10, 40, y 60 céntimos y, al menos, necesitamos 2 de cada tipo ¿Cuántos sellos de cada clase podremos comprar?

3. Llueve y, en un mercadillo improvisado en Moscú, un paraguas nos cuesta 190 rublos. Disponemos solo de billetes de 3 rublos, y el vendedor solo de 5 rublos ¿Podremos hacer la compra-venta? ¿Cómo?

4. En una torre eléctrica, se nos ha roto una pata de 4 m de altura. Para equilibrarlo provisionalmente, disponemos de 7 discos de madera de 50 cm de grosor y de otros 12 de 30 cm. ¿Cuál de las siguientes afirmaciones es verdadera?

- ☐ No podremos equilibrar la torre.
- ☐ Podremos equilibrar la torre, y de una única manera.
- ☐ Podremos equilibrar la torre, y de dos únicas maneras.
- ☐ Podremos equilibrar la torre, y de más de 2 maneras distintas.

5. Calcular el máximo común divisor y el mínimo común múltiplo, en el anillo $\mathbb{R}[x]$, de los polinomios $x^3 - 2x^2 - 5x + 6$ y $x^3 - 3x^2 - x + 3$. Encontrar todos los polinomios $f(x)$ y $g(x)$ en $\mathbb{R}[x]$, ambos de grado 3, tales que
$$(x^3 - 2x^2 - 5x + 6)f(x) + (x^3 - 3x^2 - x + 3)g(x) = x^3 - 6x^2 + 11x - 6.$$

6. Calcular el máximo común divisor y el mínimo común múltiplo, en el anillo $\mathbb{Z}_3[x]$, de los polinomios $x^4 + x^3 - x - 1$ y $x^5 + x^4 - x - 1$.Encontrar todos los polinomios $f(x)$ y $g(x)$ en $\mathbb{Z}_3[x]$, con grado de $g(x)$ igual a 7, tales que
$$(x^4 + x^3 - x - 1)f(x) + (x^5 + x^4 - x - 1)g(x) = x^4 + x^2 + 1.$$

7. a) En el anillo $\mathbb{Z}[\sqrt{-2}]$, calcular
$$(2 - 3\sqrt{-2}, 1 + \sqrt{-2}),\ [2 - 3\sqrt{-2}, 1 + \sqrt{-2}].$$

8. En $\mathbb{Z}[\sqrt{3}]$, calcula $(3 + \sqrt{3}, 2)$ y $[3 + \sqrt{3}, 2]$.

9. Determina enteros de Gauss $x, y \in \mathbb{Z}[i]$, con $N(x) \leq 18$, tales que
$$4x + (3 + 3i)y = -1 + 5i.$$

10. Resolver la siguiente ecuación en el anillo $\mathbb{Z}[\sqrt{2}]$:
$$(4 + \sqrt{2})x + (6 + 4\sqrt{2})y = \sqrt{2}.$$

5.3 Mínimo común múltiplo

Sea A un DI.

Definición 5.3.1. *Dados dos elementos $a, b \in A$, decimos que un elemento $m \in A$ es un mínimo común múltiplo (mcm, para acortar) de a y b, y escribiremos $m = mcm(a, b)$ o bien $m = [a, b]$, si tiene las siguientes dos propiedades*

1. *$a|m \wedge b|m$.*
2. *Si $a|c \wedge b|c$, entonces $m|c$.*

Ambas condiciones en conjunto significan que los múltiplos de m son exactamente los múltiplos comunes a a y b.

Como el mcd, el mcm de dos elementos, si existe, no es único. Si $m = [a, b]$, claramente lo es también cualquier asociado con m (pues tienen los mismos múltiplos). Y recíprocamente, si también $m' = [a, b]$ entonces m y m' tienen los mismos multiplos, y en particular, lo son uno del otro o, en otras palabras, se dividen mutuamente, luego m y m' son asociados. Así que m es único salvo asociados. Con esta salvedad, hablaremos de que "*m es el mcm de a y b*", abusando del artículo determinado.

Notemos que el concepto se extiende sin dificultad a un conjunto finito de elementos $a_1, ..., a_n \in A$: m es un mcm de ellos, cosa que escribiremos poniendo $m = mcm[a_1, ..., a_n]$ o bien $m = [a_1, ..., a_n]$, si:

1. $a_i|m\ \forall i = 1, ...n$ y,
2. si para un $c \in A$, $a_i|c\ \forall i = 1, ...n$, entonces $m|c$.

Las siguientes son propiedades generales, que se satisfacen siempre que existan los máximos comunes divisores que se ven involucrados en los enunciados (las igualdades hay que leerlas "salvo asociados"):

1. $[a, b] = [b, a]$.
2. Si a y a' son asociados, entonces $[a, b] = [a', b]$.
3. $[a, b] = a \Leftrightarrow b|a$. En particular $[a, 0] = 0$, $[a, 1] = a$.
4. $[[a, b], c] = [a, b, c] = [a, [b, c]]$.
5. $[ac, bc] = [a, b]c$.

   Si $c = 0$, es obvio. Supongamos $c \neq 0$. Como $c|ac$, será $c|[ac, bc]$, ya que este último es un múltiplo de ac. Pongamos $[ac, bc] = cq$. Sea $m = [a, b]$. Como $a|m$ y $b|m$, también $ac|mc$ y $ab|mc$, por tanto que $cq = [ac, bc]|mc$, de donde concluimos que $q|m$. Por otra parte, como $ac|cq = [ac, bc]$ y $bc|cq = [ac, bc]$, será $a|q$ y $b|q$, de modo que $m|q$. Luego m es asociado a q, y $q = [a, b]$. Así que $[ac, bc] = c[a, b]$.

La siguiente es muy relevante,

Teorema 5.3.2. *En un DE existe mcm de todo par de elementos. Además, para cualquier par de elementos a, b, se tiene que*

$$(a, b)[a, b] = ab.$$

Demostración. Sean $a, b \in A$. El subconjunto $aA \cap bA$ de los múltiplo comunes es un ideal. Será principal. Supongamos $aA \cap bA = mA$. Como $m \in aA$ y $m \in bA$, es $a|m$ y $b|m$. Si $a|c$ y $b|c$, entonces $c \in aA \cap bA = mA$, luego $m|c$ y $m = [a, b]$.

Para lo segundo, probamos primero que, si $(a, b) = 1$, entonces $[a, b] = ab$: Claramente $a|ab$ y $b|ab$. Si $a|c$ y $b|c$, como $(a, b) = 1$, sabemos que entonces $ab|c$.

Supongamos ahora que $(a, b) = d$. Pongamos $a = da'$ y $b = db'$, con lo que $(a', b') = 1$ y, por lo ya probado $[a', b'] = a'b'$. Pero entonces

$$(a, b)[a, d] = d[a'd, b'd] = d^2[a', b'] = d^2a'b' = (da')(db') = ab.$$

■

Observación 5.3.1. En el tema anterior definimos operaciones con ideales, aunque dejamos hacer el cálculo explícito de la suma y la intersección de ideales. Después de los Teoremas 5.1.4 y 5.3.2 tenemos que en un DE A:

- $aA + bA = (a, b)A$.
- $aA \cap bA = [a, b]A$.
- $aA \cdot bA = abA$.

5.4 Congruencias en DE

Recordemos que si $I \leq A$ es un ideal, decimos que un elemento "*a es congruente con un elemento b módulo I*", y escribimos

$$a \equiv b \mod I \qquad \text{o bien} \qquad a \equiv_I b,$$

si $a - b \in I$.

Si A es un DE, entonces todo ideal es principal, en el caso $I = mA$ hablamos simplemente de "*ser congruente módulo m*", y escribimos

$$a \equiv b \mod m \qquad \text{o bien} \qquad a \equiv_m b,$$

para significar que $a - b \in mA$ o equivalentemente, que $m|a-b$, esto es, que existe un $k \in A$ tal que $a - b = km$ o, equivalentemente, tal que $a = b + km$.

Cuando A es un Dominio Euclídeo y $m \in A$, $m \neq 0$, ser congruente módulo m está muy relacionado con lo que ocurre con el resto de dividir por m. Destacamos las siguientes propiedades:

1. Todo elemento del anillo es congruente con cualquiera de sus restos de división por el módulo m.

2. *$a \equiv_m b$ si y solo si a y b tienen un mismo resto al dividirlos por m.*
   Si $a \equiv_m b$, entonces $a = b + mk$ para un k. Si $b = mq + r$, con $r = 0$ o $\rho(r) < \rho(m)$, entonces $a = m(q+k)+r$ y r es también un resto de dividir a entre m. Reciprocamente, si $a = mp + r$ y$b = mq + r$, con $r = 0$ o $\rho(r) < \rho(m)$, entonces $a = b + m(p - q)$ y $a \equiv_m b$.

3. *Si $ac \equiv_m bc$ y $(c, m) = 1$, entonces $a \equiv_m b$.*

4. *Si $c \neq 0$, entonces $ac \equiv_{mc} bc \Leftrightarrow a \equiv_m b$.*

Ejemplos.

1. (a) $30 \equiv 6 \mod (8)$, pues $8|30 - 6 = 24$. Entonces $(+100)$ $130 \equiv 106 \mod (8)$ y (-5) $25 \equiv 1 \mod (8)$.
   (b) $166 \equiv 102 \mod (8) \Leftrightarrow 66 \equiv 2 \mod (8) \Leftrightarrow 64 \equiv 0 \mod (8) \Leftrightarrow 8|64$, ¡Sí!.
   (c) Que $30 \equiv 6 \mod (8)$ no implica que $(:6)5 \equiv 1 \mod (8)$, lo que es falso, pues $(6, 8) \neq 1$. Pero si implica que $10 \equiv 2 \mod (8)$, pues $(3, 8) = 1$.

2. *Calcular los restos módulo 7 de las potencias naturales de 2.*
   Calculemos las primeras potencias

   $$2^0 = 1 \equiv_7 1; \qquad 2^1 = 2 \equiv_7 2; \qquad 2^2 = 4 \equiv_7 4; \qquad 2^3 = 8 \equiv_7 1.$$

   Ya hay una repetición. Ya se van a repetir todas: Si $n \equiv 0 \mod (3)$, entonces $n = 3k$, y $2^n = (2^3)^k \equiv_7 1^k = 1$; luego el resto de dividir 2^n entre siete será 1. Si $n \equiv 1 \mod (3)$, entonces $n = 3k + 1$, y $2^n = (2^3)^k 2 \equiv_7 1^k 2 = 2$; luego el resto de dividir 2^n entre siete será 2. Si $n \equiv 2 \mod (3)$, entonces $n = 3k + 2$, y $2^n = (2^3)^k 2^2 \equiv_7 1^k 4 = 4$; luego el resto de dividir 2^n entre siete será 4. Como todo número es congruente con 0, 1 o 2 módulo 3 (su resto al dividirlo 3), ya los tenemos todos.

Por ejemplo, ¿Qué resto da 2^{350} al dividirlo por 7? Será 4, pues

$$350 = 10 \cdot 35 = 10 \cdot 5 \cdot 7 \equiv_7 1 \cdot 2 \cdot 1 = 2.$$

3. Calcular el resto de dividir $100^{1034} + 30^{3147}125^{311}$ entre 7.

   Como $100 = 2 \cdot 50 \equiv_7 2 \cdot 1 = 2$, $100^{1034} \equiv_7 2^{1035}$. Como $1034 = 1000 + 34 \equiv_3 1 + 1 = 2$, concluimos que $100^{1034} \equiv_7 4$.

   Como $30^{3147} \equiv_7 2^{3147} = 2^{15} \equiv_7 2^{3\cdot 1049} \equiv_7 1$, y $125^{311} = (5^3)^{311} \equiv_7 ((-2)^3)^{311} = -(2^3)^{311} \equiv_7 (-1)^{311} = -1$, concluimos que

   $$100^{1034} + 30^{3147} + 125^{311} \equiv_7 4 + 1 - 1 = 4.$$

4. Argumentar que un número natural es congruente módulo 3 con la suma de sus cifras. En particular divisible por 3 si y solo si lo es la suma de sus cifras.

   Si $n = a_m a_{m-1} \cdots a_1 a_0$, con $0 \leq a_i \leq 9$, $a_m \neq 0$, entonces $n = a_0 + a_1 10 + a_2 10^2 + \cdots + a_m 10^m$ y, como $10 \equiv_3 1$, $n \equiv_3 a_0 + a_1 + \cdots + a_m$.

4. Calcular el resto de dividir 13912 entre 3.

   $13913 \equiv_3 17 \equiv_3 8 \equiv_3 2$.

La siguiente observación es general para potencias en congruencias entre números enteros.

Lema 5.4.1. *Si* $a^e \equiv a^{e+k} \mod (m)$, *entonces, para cualquier* $n \geq 0$,

$$a^{e+n} \equiv a^{e+r} \mod (m)$$

donde r *es el resto de dividir* n *entre* k. *Par tanto, las potencias de* a *son congruentes, módulo* m, *con* $1 = a^0, a, a^2, \ldots, a^e, a^{e+1}, \ldots, a^{e+k-1}$.

En particular, si $e = 0$, *esto es, si* $a^k \equiv 1 \mod (m)$, *entonces, para cualquier* $n \geq 0$,

$$a^n \equiv a^r \mod (m)$$

donde r *es el resto de dividir* n *entre* k. *Par tanto, las potencias de* a *son congruentes, módulo* m, *con* $1, a, a^2, \ldots, a^{k-1}$.

Demostración. Vemos primero, por inducción en $q \geq 0$, que $a^{e+qk} \equiv a^e \mod (m)$. Para $q = 0$ es evidente. Entonces, supuesto para q,

$$a^{e+k(q+1)} = a^{e+kq}a^k \equiv_m a^e a^k \equiv_m a^{e+k} \equiv_m a^e.$$

Entonces, si $n = kq + r$, con $0 \leq r < k$, $a^{e+n} = a^{e+kq+r} = a^{e+kq}a^r \equiv_m a^e a^r = a^{e+r}$. ■

EJEMPLO. *Calcular el resto de* $2^{(47^{51})}$ *módulo* 14.

Empezamos las primeras potencias de 2: $2^0 \equiv_{14} 1$, $2^1 \equiv_{14} 2$, $2^3 \equiv_{14} 8$, $2^4 \equiv_{14} 16 \equiv_{14} 2$. Así que $2^1 \equiv_{14} 2^{1+3}$, luego, para cualquier $n \geq 0$, $2^{n+1} \equiv_{14} 2^{r+1}$, si r es el resto de dividir n entre 3. Calculemos entonces el resto de dividir $47^{51} - 1$ entre 3:

$$47^{51} - 1 \equiv_3 11^{51} - 1 \equiv_3 2^{51} - 1 \equiv_3 (-1)^{51} - 1 \equiv_3 -2 \equiv_3 1.$$

Luego, $2^{(47^{51})} \equiv_{14} 2^{1+1} = 4$.

5.4.1 La ecuación básica $ax \equiv b \mod m$

Nos situamos en el contexto de ser A un DE.

Teorema 5.4.2. *Sea la ecuación $ax \equiv b \mod m$, con $m \neq 0$, y supongamos que $d = (a, m)$.*

1. *La ecuación tiene solución si y solo si $d|b$.*
2. *Si $d|b$, y $a = da'$, $b = db'$ y $m = dm'$, la ecuación es equivalente a la ecuación "reducida"*
$$a'x \equiv b' \mod (m').$$
3. *Si $d|b$, y x_0 es cualquier solución particular, la ecuación original es equivalente a la ecuación*
$$x \equiv x_0 \mod (m').$$
Esto es, la solución general es $x = x_0 + km'$, $k \in A$.
4. *Hay una solución x_0 tal que $x_0 = 0$ o, en otro caso, $\rho(x_0) < \rho(m')$, la que llamaremos "solución óptima".*

Demostración.

1. La ecuación tiene solución si y solo si existe un y tal que $ax - my = b$, ecuación diofántica que tiene solución si y solo si $d|b$.
2. Un x verifica la ecuación si y solo si verifica que $da'x \equiv db' \mod dm'$, lo que se verifica si y solo si $a'x \equiv b' \mod m'$.
3. Como $(a', m') = 1$, podemos encontrar u, v tal que $1 = a'u + m'v$. Entonces $a'u \equiv 1 \mod m'$ y, por tanto, $a'b'u \equiv b' \mod m'$. Luego $x_0 = b'u$ es una solución particular. Si x es cualquier elemento con $x \equiv x_0 \mod m'$, entonces $a'x \equiv a'x_0 \mod m'$ y, por tanto, también $a'x \equiv b' \mod m'$. Y, reciprocamente, si $a'x \equiv b' \mod m'$, entonces $a'x \equiv a'x_0 \mod m'$. Como $(a', m') = 1$, necesariamente será $x \equiv x_0 \mod m'$.
4. Si x_0' es un resto de dividir cualquier solución particular previamente obtenida x_0 entre m', tendremos que $x_0 \equiv x_0' \mod m'$, entonces también que $a'x_0' \equiv b' \mod m'$, donde $x_0' = 0$ o $\rho(x_0') < \rho(m')$.

■

Observación 5.4.1. Si en la ecuación reducida $a'x \equiv b' \mod m'$, existe un c tal que $c|a'$ y $c|b'$, y ponemos $a' = ca''$ y $b' = cb''$, entonces la ecuación se escribe como $ca''x \equiv cb'' \mod m'$ y es equivalente, ya que $(c, m') = 1$, a la ecuación

$$a''x \equiv b'' \mod m'.$$

Ejemplos.

1. Resolver la ecuación en $\mathbb{Z}$: $60x \equiv 90 \mod 105$.

Como $(60, 105) = 5(12, 21) = 15(4, 7) = 15$ y $90 = 15 \cdot 6$, la ecuación tiene solución. Esta resulta equivalente a s "reducida": $4x \equiv 6 \mod 7$. Como $1 = 7 \cdot (-1) + 4 \cdot 2$, resulta que $4 \cdot \equiv 1 \mod (7)$ y entonces $4 \cdot 12 \equiv 6 \mod (7)$. Luego 12 es una solución particular y $12 \equiv 5 \mod 7$, 5 es la óptima. La ecuación original es equivalente a $x \equiv 5 \mod 7$ y la solución general óptima $x = 5 + 7k$, $k \in \mathbb{Z}$.

2. Resolver la ecuación en $\mathbb{Z}$: $1100x \equiv 660 \mod 140$.

La ecuación es equivalente a $110x \equiv 66 \mod 14$; también a $55x \equiv 33 \mod 7$, a $5x \equiv 3 \mod 7$, a $-2x \equiv -4 \mod 7$, y a $x \equiv 2 \mod 7$.

3. Resolver la ecuación en $\mathbb{Z}[\sqrt{2}]$: $(2+\sqrt{2})x \equiv 3-\sqrt{2} \mod 3$.

La tabla

$$\begin{array}{ccc|cc} & 3 & & 1 & 0 \\ & 2+\sqrt{2} & & 0 & 1 \\ 3-\sqrt{2} & -1-\sqrt{2} & & 1 & -3+\sqrt{2} \\ & 0 & & & \end{array},$$

nos indica que $(2+\sqrt{2}, 3) = -1-\sqrt{2}$, que es unidad con $(-1-\sqrt{2})^{-1} = 1-\sqrt{2}$.

De la igualdad $-1-\sqrt{2} = 3\cdot(1)+(2+\sqrt{2})(-3+\sqrt{2})$, obtenemos que $(2+\sqrt{2})(-3+\sqrt{2}) \equiv -1-\sqrt{2} \mod (3)$ y, multiplicando por $1-\sqrt{2}$, que $(2+\sqrt{2})(-5+4\sqrt{2}) \equiv 1 \mod 3$. Entonces, multiplicando por $3-\sqrt{2}$, obtenemos que $(2+\sqrt{2})(-23+17\sqrt{2}) \equiv 3-\sqrt{2} \mod 3$, y una solución particular es $-23+17\sqrt{2}$. Sus resto al dividirlo por 3 es $1-\sqrt{2}$, la ecuación original es equivalente a $x \equiv 1-\sqrt{2} \mod (3)$.

El estudio de estas ecuaciones tiene su repercusión en el estudio de unidades de anillos cocientes de un DE.

Teorema 5.4.3. *Sea A un DE y $m \in A$, no nulo ni unidad.*

1. *Un elemento $\bar{a} \in A/mA$ es una unidad si y solo si $(a, m) = 1$.*
2. *El anillo cociente A/mA es un DI $\Leftrightarrow$ es un cuerpo $\Leftrightarrow$ m es irreducible.*

Demostración.

1. El elemento $\bar{a}$ es una unidad en A/mA si y solo si $\exists x \in A$ tal que $\bar{a}\bar{x} = \bar{1}$; esto es, si y solo si la congruencia $ax \equiv 1 \mod m$ tiene solución, lo que sabemos ocurre si y solo si $(a, m) = 1$. Notemos que, en tal caso, $\bar{a}^{-1} = \bar{x}$, donde $ax \equiv 1 \mod m$.
2. Supongamos que m es irreducible. Si $\bar{a} \in A/mA$ no es nulo, o sea $\bar{a} \neq \bar{0}$, entonces a no es múltiplo de m y es $(a, m) = 1$. Luego $\bar{a} \in U(A/mA)$ por (1). Ya sabemos que si A/mA es cuerpo entonces es un DI. Finalmente, si m no es irreducible, será $m = ab$ en A, donde ninguno es múltiplo de m. Pero entonces, en A/mA $0 = \bar{m} = \bar{a}\bar{b}$ con $\bar{a} \neq \bar{0} \neq \bar{b}$ y, por tanto, A/mA no es DI.

■

Podemos particularizar el Teorema 5.4.3 al caso de DE ya estudiados, recordar que habíamos identificado el anillo de restos módulo n, $\mathbb{Z}_n$ con el anillo cociente $\mathbb{Z}/n\mathbb{Z}$.

Corolario 5.4.4.

(*i*) *$\mathbb{Z}_n$ es un cuerpo $\Leftrightarrow$ n es un irreducible.*

(*ii*) *$K[x]/\langle f\rangle$ es un cuerpo $\Leftrightarrow$ f es un polinomio irreducible.*

(*iii*) *Si $n = -2, -1, 2, 3$ y $\alpha \in \mathbb{Z}[\sqrt{n}]$, entonces $\mathbb{Z}[\sqrt{n}]/\langle\alpha\rangle$ es un cuerpo $\Leftrightarrow$ α es irreducible.*

Observación 5.4.2.

Si $p \geq 2$ es un irreducible de $\mathbb{Z}$ y $f = a_0 + a_1x + \cdot + a_nx^n$, con $a_n \neq 0$ es un irreducible de $\mathbb{Z}_p[x]$, el cuerpo $Z_p[x]/\langle f\rangle$ tiene exactamente p^n elementos, en efecto:

Si $\bar{g} \in \mathbb{Z}_p[x]/\langle f\rangle$, y $r = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ es el resto de dividir g entre f, entonces $\bar{g} = \bar{r}$. Así, toda clase de congruencia en $\mathbb{Z}_p[x]/\langle f\rangle$ está representada por un polinomio de la

forma $b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$, esto es, de grado menor que n. Dos polinomios de estos no pueden ser congruentes módulo f, pues este tiene grado n. Así que en $\mathbb{Z}_p[x]/\langle f\rangle$ hay tantos elementos distintos como polinomios en $Z_p[x]$ de la forma $b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$. En total p^n. Se denota a este cuerpo $\mathbb{F}_{p^n}$, y os menciono aquí que en cursos superiores veréis el Teorema de Moore, que asegura que, salvo isomorfismo, *estos son los únicos cuerpos finitos que existen.*

5.4.2 Sistemas de 2 congruencias en un DE

Vamos a estudiar el sistema de congruencias

$$\begin{cases} a_1x \equiv b_1 \mod m_1 \\ a_2x \equiv b_2 \mod m_2 \end{cases}$$

Puesto que cada ecuación ha de tener solución, un tal sistema será siempre equivalente a uno de la forma

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n, \end{cases} \tag{5.1}$$

cuya discusión nos lleva a la siguiente conclusión.

Teorema 5.4.5. *El sistema* (5.1) *tiene solución si y solo si* $a \equiv b \mod (m,n)$.

En tal caso, existe una solución x_0 *tal que, si* $x_0 \neq 0$, *entonces* $\rho(x_0) < \rho([m,n])$, *a la llamamos solución "*óptima*", y la solución general es*

$$x = x_0 + k[m,n] \qquad (k \in A).$$

Esto es, el sistema de ecuaciones original es equivalente a la ecuación

$$x \equiv x_0 \mod [m,n].$$

Demostración. Para que una solución $x = a + tm$ de la primera en (5.1) lo sea también de la segunda será por que $mt \equiv b - a \mod n$; y un tal t existe si y solo si $(m,n)|b-a$. Esto es, si y solo si $a \equiv b \mod (m,n)$. Además, si t_0 es cualquier solución particular de esta última, la solución general de esta será de la forma $t = t_0 + k\frac{n}{(m,n)}$, con $k \in A$. Luego la general del sistema es

$$x = a + tm = a + \Big(t_0 + k\frac{n}{(m,n)}\Big)m = a + t_0m + k[m,n] \qquad (k \in A).$$

En otros términos, el sistema es equivalente a la simple ecuación $x \equiv (a + t_0m) \mod [m,n]$. Si consideremos entonces x_0 el resto de dividir $a + t_0m$, concluimos que, la solución general es

$$x \equiv x_0 \mod [m,n]$$

donde $x_0 = 0$ o $\rho(x_0) < \rho([m,n])$. ■

Ejemplo. Tengo depósitos cuya capacidad no excede de 100 litros. Al llenar 6 de ellos con bidones de 11 litros, me sobraron 8. Al llenar 5 con bidones de 23, me sobraron 15 ¿qué capacidad tienen mis depósitos?.

El sistema a resolver es

$$\begin{cases} 6x \equiv 8 \mod 11 \\ 5x \equiv 15 \mod 23 \end{cases} \sim \begin{cases} x \equiv 5 \mod 11 \\ x \equiv 3 \mod 23 \end{cases}.$$

Buscamos los $x = 5 + 11t$ tales que $5 + 11t \equiv 3 \mod 23$, o sea, tales que $11t \equiv -2 \mod 23$. Multiplicando por 2, está ecuación es equivalente a $-t \equiv -4 \mod 23$, o sea a $t \equiv 4 \mod 23$. Una solución particular es $x_0 = 5 + 44 = 49$ y la general $x \equiv 49 \mod [11,23]$; esto es, $x \equiv 49 \mod (253)$, o $x = 49 + 253k$, $k \in \mathbb{Z}$. Total: 49 litros es la capacidad de mis depósitos.

5.4.3 Sistemas de r congruencias

Para resolver un sistema con $r \geq 3$ ecuaciones

$$\begin{cases} a_1 x \equiv b_1 & \mod m_1 \\ a_2 x \equiv b_2 & \mod m_2 \\ a_3 x \equiv b_3 & \mod m_3 \\ \cdots & \\ a_r x \equiv b_r & \mod m_r \end{cases}$$

procedemos como sigue. Resolvemos primero cada una, y el sistema, si todas tienen solución, se re-escribirá en la forma

$$\begin{cases} x \equiv c_1 & \mod m_1 \\ x \equiv c_2 & \mod m_2 \\ x \equiv c_3 & \mod m_3 \\ \cdots & \\ x \equiv c_r & \mod m_r \end{cases}$$

Resolvemos entonces el sistema formado por las dos primeras. Si tiene solución, este sistema resultará equivalente a una simple ecuación de la forma $x \equiv c \mod m$. Luego el sistema original de r ecuaciones será equivalente al sistema formado por las $r-1$ ecuaciones

$$\begin{cases} x \equiv c & \mod m \\ x \equiv c_3 & \mod m_3 \\ \cdots & \\ x \equiv c_r & \mod m_r \end{cases}$$

y reiteramos el proceso, resolviendo el sistema de las dos primeras, hasta concluir con una sola, que será de la forma $x \equiv d \mod n$, que ya expresará la solución general del sistema inicial: $x = d + kn$, con $k \in A$.

Ejemplo. Determinar los polinomios $f \in \mathbb{Q}[x]$ tales que

1. $gr(f) \leq 3$.
2. $f(1) = 8$,
3. $f(-1) = 2$,
4. El resto de dividir f entre $x^2 + 1$ es $x + 1$.

Recordemos el teorema de Ruffini: Si $f \in K[x]$ y $a \in K$, entonces $f(a)$ es el resto de dividir f entre $x - a$". En efecto, será $f = q(x-a) + r$, donde $r \in K$. Pero entonces $f(a) = r$.

En otras palabras, el Teorema de Ruffini nos dice que $f \equiv f(a) \mod (x-a)$, para cualquier $a \in K$.

Buscamos entonces los polinomios de grado 3 que satisfacen el sistema

$$\begin{cases} f \equiv 8 & \mod (x-1), \\ f \equiv 2 & \mod (x+1) \\ f \equiv x+1 & \mod (x^2+1). \end{cases}$$

Procedemos: $f = 8 + t(x-1)$; $8 + t(x-1) \equiv 2 \mod (x+1)$; $(x-1)t \equiv -6 \mod (x+1)$; De la tabla

$x-1$	1	0
$x+1$	0	1
-2	1	-1
0		

,

obtenemos que $-2 = (x-1) \cdot 1 + (x+1) \cdot (-1)$. Luego $(x-1) \cdot 1 \equiv -2 \mod (x+1)$, y $(x-1) \cdot (-\frac{1}{2}) \equiv 1 \mod (x+1)$. Entonces, $(x-1)(-\frac{1}{2})(-6) \equiv (-6) \mod (x+1)$ y una solución particular es $t_0 = 3$. El sistema formado por las dos primeras ecuaciones es equivalente a la ecuación $f \equiv 8 + 3(x-1) \mod (x^2-1)$; esto es $f \equiv 3x + 5 \mod (x^2-1)$.

La solución general de la última es $f = (x+1) + t(x^2+1)$, y nos planteamos entonces la ecuación

$$(x+1) + t(x^2+1) \equiv 3x + 5 \mod (x^2-1)$$

o, equivalentemente,

$$(x^2+1)t \equiv 2x + 4 \mod (x^2-1).$$

De la tabla

x^2+1	1	0
x^2-1	0	1
2	1	-1
0		

obtenemos $2 = (x^2+1)\cdot 1 + (x^2-1)\cdot(-1)$ y $1 = (x^2+1)\cdot(\frac{1}{2}) + (x^2-1)\cdot(-\frac{1}{2})$. Así que $(x^2+1)\cdot\frac{1}{2} \equiv 1 \mod (x^2-1)$ y $(x^2+1)\cdot(x+2) \equiv 2x+4 \mod (x^2-1)$. Luego una solución particular es $t_0 = x+2$ y $f_0 = (x+1) + (x+2)(x^2+1) = x^3 + 2x^2 + 2x + 3$ es una solución particular al sistema de las dos ecuaciones. El sistema general es entonces equivalente a $f \equiv x^3 + 2x^2 + 2x + 3 + \mod (x^4+1)$. En definitiva, el polinomio buscado es $f = x^3 + 2x^2 + 2x + 3$.

5.5 Complementos sobre $\mathbb{Z}_n$

5.5.1 La ecuación $ax = b$ en $\mathbb{Z}_n$

Sea $n \geq 2$ un entero, y consideremos la ecuación $ax = b$ en el anillo $\mathbb{Z}_n$, donde $a \neq 0$.

El conjunto de sus soluciones será

$$\begin{aligned}\{x \in \mathbb{Z};\ 0 \leq x < n,\ ax = b \text{ en } \mathbb{Z}_n\} &= \{x \in \mathbb{Z};\ 0 \leq x < n,\ \overline{ax} = \bar{b} \text{ en } \mathbb{Z}/n\mathbb{Z}\} \\ &= \{x \in \mathbb{Z} \mid 0 \leq x < n,\ ax \equiv b \mod n\}\end{aligned}$$

Si $d = (a,n)$ no divide a b, la ecuación no tiene solución.

Supongamos que $d|b$, sabemos que la ecuación $ax \equiv b \mod n$ tiene solución, y más aun, que tiene una solución x_0 óptima, satisfaciendo que $0 \leq x_0 < n' = \frac{n}{d}$. Además todas las soluciones de la congruencia $ax \equiv b \mod n$ son entonces los $x = x_0 + kn'$, con $k \in \mathbb{Z}$. Concluimos entonces

Proposición 5.5.1. *Si $d|b$ hay d diferentes soluciones de la ecuación $ax = b$ en $\mathbb{Z}_n$ que son:*

$$\{x_0, x_0 + n', x_0 + 2n', \ldots, x_0 + (d-1)n'\}.$$

Demostración. Estas son efectivamente soluciones de la congruencia $ax \equiv b \mod (n)$, y para cualquier $0 \leq k < d$, se satisface que $x_0 + kn' < n' + (d-1)n' = dn' = n$. Y no hay más, pues para cualquier $k \in \mathbb{Z}$, si $k < 0$, entonces $x_0 + kn' < 0$; y si $k \geq d$, entonces $x_0 + kn' \geq x_0 + dn' \geq dn' = n$.

Observar también que, si $(a,n) = 1$, la ecuación $ax = 1$ en $\mathbb{Z}_n$ siempre tiene solución, y esta es única es única: $x_0 = a^{-1}$. ■

Ejemplo. *Resolver la ecuación $12x = 18$ en $\mathbb{Z}_{30}$.* Como $(12,30) = 6(2,5) = 6$ y $6/18$, la ecuación tiene 6 soluciones. Para buscarlas consideramos la ecuación $12x \equiv 18 \mod (30)$, que reduce a $2x \equiv 3 \mod (5)$. Fácilmente se ve que $x_0 = 4$ es la solución óptima. Pero podemos llegar a ella aplicando el procedimiento ortodoxo:

5	1	0
2	0	1
1	1	-2

así que $1 = 1 \cdot 5 + 2 \cdot (-2)$, de donde $2 \cdot (-2) \equiv 1 \mod (5)$, o lo que es lo mismo $2 \cdot 3 \equiv 1 \mod (5)$. Entonces $2 \cdot 9 \equiv 3 \mod (5)$ y $2 \cdot 4 \equiv 3 \mod (5)$. Luego $x_0 = 4$ es solución y óptima. El conjunto de todas las soluciones sería

$$\{4 + k5, k = 0, \dots 4\} = \{4, 9, 14, 19, 24, 29\}.$$

5.5.2 La función φ de Euler

Se define como la aplicación

$$\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\},$$

que asigna como imagen de cada numero natural $n \geq 1$ el número natural

$$\varphi(n) = |\{m \mid 1 \leq m \leq n, (m, n) = 1\}|.$$

Como ejemplo, tenemos que

$$\varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(5) = 4, \quad \varphi(6) = 2, ...$$

y vemos que no sigue una pauta clara. Las siguientes observaciones van dirigidas a mostrar como se puede calcular $\varphi(n)$, para los diferentes n.

En principio, $\varphi(n)$ tiene la siguiente interpretación.

Proposición 5.5.2. *para cada $n \geq 2$,*

$$\varphi(n) = |U(\mathbb{Z}_n)|.$$

Demostración. $U(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n \mid \exists x \in \mathbb{Z}_n \text{ con } ax = 1\} = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$. ■

Lema 5.5.3. *Sea $f : A \cong B$ es un isomorfismo de anillos, entonces la aplicación restringida $f : U(A) \to U(B)$, que asigna a cada unidad a su imagen por f, $f(a)$, es una biyección.*

Demostración. La aplicación $f : U(A) \to U(B)$ es claramente inyectiva. Si $b \in U(B)$, existirán un $a, a' \in A$ tales que $f(a) = b$ y $f(a') = b^{-1}$. Pero entonces $f(aa') = f(a)f(a') = bb^{-1} = 1 = f(1)$, luego $aa' = 1$, pues f es inyectiva. Entonces $a \in U(a)$ y $f(a)) = b$. ■

Si A y B son anillos conmutativos, se define su "*anillo producto*" como el producto cartesiano $A \times B$, con las operaciones

$$(a, b) + (a', b') = (a + a', b + b'), \quad (a, b)(a', b') = (aa', bb').$$

La verificación de los axiomas es fácil. Su cero es el par $(0, 0)$, y su uno el par $(1, 1)$. El opuesto de un par (a, b) es el par $(-a, -b)$. Además,

Lema 5.5.4. $U(A \times B) = U(A) \times U(B)$.

Demostración. Para cada $(a, b) \in A \times B$, se tiene que

$$\begin{aligned}(a, b) \in U(A \times B) &\Leftrightarrow \exists (a', b') \mid (aa', bb') = (1, 1) \Leftrightarrow a \in U(A) \wedge b \in U(B) \\ &\Leftrightarrow (a, b) \in U(A) \times U(B).\end{aligned}$$

■

Lema 5.5.5 (Teorema Chino del resto)**.**
Si $m, n \geq 2$, son enteros con $(m, n) = 1$, entonces hay un isomorfismo

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

que hace corresponder a cada $k \in \mathbb{Z}_{mn}$ su par de restos $(R_m(k), R_n(k))$ al ser dividido por m y n respectivamente.

Demostración. Sea $f : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ la aplicación que asigna a cada $x \in \mathbb{Z}$ el par $(R_m(x), R_n(x))$ de sus restos en $\mathbb{Z}_m$ y $\mathbb{Z}_n$ respectivamente. Es fácil ver que R es un homomorfismo de anillos, desde que $R_m : \mathbb{Z} \to \mathbb{Z}_m$ y $R_n : A \to A_n$ lo son.

Veamos que es un epimorfismo:

Para cualquier $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, el sistema de ecuaciones en congruencias en $\mathbb{Z}$

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

tiene solución, pues $(m, n) = 1 | a - b$. Existe por tanto un $x \in A$ satisfaciendo ambas congruencias. Pero entonces $R_m(x) = a$ y $R_n(x) = b$; esto es $f(x) = (a, b)$.

El núcleo de f consiste de todos los $x \in \mathbb{Z}$ tal que $R_m(x) = 0$ y $R_n(x) = 0$, esto es, tales que $x \equiv 0 \mod m$ y $x \equiv 0 \mod m$. En otras palabras, los $x \in \mathbb{Z}$ tales que $m|x$ y $n|x$, que es lo mismo que decir que $[m, n] = mn|x$. Así que $Ker(f) = mn\mathbb{Z}$ es el ideal de los múltiplos de mn. El Primer Teorema de Isomorfía, nos asegura entonces que f induce in isomorfismo

$$\bar{f} : \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}_m \times \mathbb{Z}_n,$$

definido por $\bar{f}(\bar{x}) = f(x) = (R_m(x), R_n(x))$. Componiendo este con el isomorfismo $\mathbb{Z}_{mn} \cong \mathbb{Z}/mn\mathbb{Z}$, que asigna a cada $x \in \mathbb{Z}_{mn}$ su clase de congruencia $\bar{x}$ en $\mathbb{Z}/mn\mathbb{Z}$, obtenemos el isomorfismo buscado $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, que asigna a cada $x \in \mathbb{Z}_{mn}$ el par de restos $(R_m(x), R_n(x))$. ■

Lema 5.5.6. *Si $m, n \geq 2$ son enteros con $(m, n) = 1$, entonces $\varphi(mn) = \varphi(m)\varphi(n)$.*

Demostración. Para tales enteros m, n se tiene que
$\varphi(mn) = |U(\mathbb{Z}_{mn}| = |U(\mathbb{Z}_m \times \mathbb{Z}_n)| = |U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)| = |U(\mathbb{Z}_m)||U(\mathbb{Z}_n)| = \varphi(m)\varphi(n)$. ■

Lema 5.5.7. *Si $p \geq 2$ es un número irreducible, para cada $e \geq 1$,*

$$\varphi(p^e) = p^e\Big(1 - \frac{1}{p}\Big).$$

Demostración. Para cualquier natural m, si p/m, entonces $p/(p^e, m)$ y, por tanto, $(p^e, m) \neq 1$. En otro caso, si p no divide a m, entonces ninguna potencia de p lo hace. Como os únicos divisores de p^e son, salvo signo, potencias de p, el único divisor común a p^e y m es 1, salvo el signo, y $(p^e, m) = 1$. Por tanto, los naturales m con $1 \leq m \leq p^e$ y $(p^e, m) \neq 1$, son los de la forma kp, con $p = 1 \cdot p \leq kp \leq p^e = p^{e-1}p$, esto es, con $1 \leq k \leq p^{e-1}$. El número de estos es p^{e-1} y, en consecuencia, los naturales m con $1 \leq m \leq p^e$ y $(p^e, m) = 1$ están en número

$$p^e - p^{e-1} = p^{e-1}(p - 1) = p^e\Big(1 - \frac{1}{p}\Big).$$

■

Teorema 5.5.8. *Si $p_1, \cdots, p_r$ son los diferentes irreducibles que dividen al natural $n \geq 2$, entonces*

$$\varphi(n) = n\Big(1 - \frac{1}{p_1}\Big)\cdots\Big(1 - \frac{1}{p_r}\Big).$$

Demostración. Sea $n = p_1^{e_1}\cdots p_r^{e_r}$, la factorización de n en producto de irreducibles, con $p_i \neq p_j$. Hagamos inducción en r. Si $r = 1$, la fórmula ha sido probada antes. Supuesto $r > 1$, hacemos hipótesis de inducción. Sea $m = p_2^{e_1}\cdots p_r^{e_r}$. Entonces $(p_1^{e_1}, m) = 1$ y, por tanto,

$$\varphi(n) = \varphi(p_1^{e_1})\varphi(m) = p_1^{e_1}\Big(1 - \frac{1}{p_1}\Big)m\Big(1 - \frac{1}{p_2}\Big)\cdots\Big(1 - \frac{1}{p_r}\Big) = n\Big(1 - \frac{1}{p_1}\Big)\cdots\Big(1 - \frac{1}{p_r}\Big).\square$$

■

Ejemplo.

$$\varphi(10) = 10\Big(1 - \frac{1}{2}\Big)\Big(1 - \frac{1}{5}\Big) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4.$$

$$\varphi(36) = 36\Big(1 - \frac{1}{2}\Big)\Big(1 - \frac{1}{3}\Big) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12.$$

Concluimos con la siguiente consecuencia

Teorema 5.5.9 (Fermat)**.** *Sea $n \geq 2$ un entero.*

1. *Para cualquier $a \in \mathbb{Z}$ tal que $(a, n) = 1$, se verifica que $a^{\varphi(n)} \equiv 1 \mod (n)$.*
2. *Si p es irreducible, para cualquier $a \in \mathbb{Z}$ que no es divisible por p se tiene que $a^{p-1} \equiv 1 \mod (p)$ y $a^p \equiv a \mod (p)$.*
3. *Para cualquier $r \in U(\mathbb{Z}_n)$, es decir, tal que $(r, n) = 1$, se verifica que $r^{\varphi(n)} = 1$ en el anillo $\mathbb{Z}_n$. Entonces $r^{-1} = r^{\varphi(n)-1}$.*
4. *Si $n = p$ es irreducible, para cualquier r en el cuerpo $\mathbb{Z}_p$ se tiene que $r^{p-1} = 1$ y $r^p = r$.*

Demostración.

(3) Tenemos que $r \in U(\mathbb{Z}_n)$. Sea $x = \prod_{m\in U(\mathbb{Z}_n)} m$, el producto en $\mathbb{Z}_n$ de todas sus unidades. La aplicación $f : U(\mathbb{Z}_n) \to U(\mathbb{Z}_n)$ tal que $f(m) = rm$, es claramente inyectiva y, entonces, biyectiva. Así que $U(\mathbb{Z}_n) = \{rm, m \in U(\mathbb{Z}_n)\}$. Por tanto

$$x = \prod_{m\in U(\mathbb{Z}_n)} m = \prod_{m\in U(\mathbb{Z}_n)} rm = r^{\varphi(n)} \prod_{m\in U(\mathbb{Z}_n)} m = r^{\varphi(n)}x.$$

Como x es una unidad, eso implica que $r^{\varphi(n)} = 1$.

(1) Consideremos el isomorfismo $\bar{R} : \mathbb{Z}/n \cong \mathbb{Z}_n$, $\bar{a} \mapsto R(a)$. Como $\bar{a} \in U(\mathbb{Z}/n)$, será $R(a) \in U(\mathbb{Z}_n)$. Entonces $R(\overline{a^{\varphi(n)}}) = R(a)^{\varphi(n)} = 1$. Luego $a^{\varphi(n)} \equiv_m 1$.

(2) y (4) son consecuencia directa de (1) y (3).

■

EJEMPLOS.

1. *Calcular* $3^{(3^{100})}$ *en* $\mathbb{Z}_{100}$.

Como $(3, 100) = 1$ y $\varphi(100) = 40$, podemos asegurar que $3^{40} \equiv 1 \mod (100)$. Busquemos el resto de dividir 3^{100} por 40: Como $(3, 40) = 1$ y $\varphi(40) = 16$, tenemos que $3^{16} \equiv 1 \mod (40)$. Como $100 = 10 \cdot 10 \equiv_{16} (-6)(-6) = 36 \equiv_{16} 4$, podemos asegurar que $3^{100} \equiv_{40} 3^4 = 81 \equiv_{40} 1$. Finalmente entonces, $3^{(3^{100})} \equiv_{100} 3^1 = 3$. □

2. *Calcular el resto de dividir* $24^{(47)^{51}}$ *entre* 14.

Puesto que $24 \equiv 10 \mod (14)$, la cuestión es lo mismo que calcular $10^{(47)^{51}}$ en $\mathbb{Z}_{14}$. Notemos que $10^{(47)^{51}} = 5^{(47^{51})}2^{(47^{51})}$, y podemos trabajar con cada factor por separado.

Como $(5, 14) = 1$, y $\varphi(14) = 6$, será $5^6 \cong_{14} 1$. Entonces, Si r es el resto de dividir 47^{51} entre 6, será $5^{(47)^{51}} \equiv_{14} 5^r$. Ahora, $47^{51} \equiv_6 5^{51}$. Ademas, como $(5, 6) = 1$ y $\varphi(6) = 2$, tendremos que $5^2 \equiv_6 1$. Entonces, como $51 \equiv_2 1$, será $5^{51} \equiv_6 5$. Por tanto

$$5^{(47^{51})} \equiv_{14} 5^5 \equiv_{14} (5^2)^2 5 \equiv_{14} (-3)^2 5 \equiv_{14} 9 \cdot 5 \equiv_{>14} (-5)5 \equiv_{14} -25 \equiv_{14} 3.$$

Para calcular el resto de $2^{(47^{51})}$ módulo 14, empezamos las primeras potencias de 2: $2^0 \equiv_{14} 1$, $2^1 \equiv_{14} 2$, $2^3 \equiv_{14} 8$, $2^4 \equiv_{14} 16 \equiv_{14} 2$. Así que $2^1 \equiv_{14} 2^{1+3}$, luego, para cualquier $n \geq 0$, $2^{n+1} \equiv_{14} 2^{r+1}$, si r es el resto de dividir n entre 3. Calculemos entonces el resto de dividir $47^{51} - 1$ entre 3:

$$47^{51} - 1 \equiv_3 11^{51} - 1 \equiv_3 2^{51} - 1 \equiv_3 (-1)^{51} - 1 \equiv_3 -2 \equiv_3 1.$$

Luego, $2^{(47^{51})} \equiv_{14} 2^{1+1} = 4$.

En definitiva, $24^{(47)^{51}} \equiv_{14} 3 \cdot 4 = 12$. □

Ejercicio 1 Resuelve las ecuaciones siguientes

1. $12x = 8$ en el anillo $\mathbb{Z}_{20}$.
2. $19x = 42$ en $\mathbb{Z}_{50}$.
3. $9x = 4$ en $\mathbb{Z}_{1453}$.
4. $5^{30}x = 2$ en $\mathbb{Z}_7$.
5. $20x = 984$ en $\mathbb{Z}_{1984}$.

Ejercicio 2 Determina, si existen, los inversos de

1. 15 en $\mathbb{Z}_{16}$.
2. 9 en $\mathbb{Z}_{20}$.
3. 12 en $\mathbb{Z}_{21}$.
4. 22 en $\mathbb{Z}_{31}$.

Ejercicio 3 Determina cuántas unidades tienen los anillos

1. $\mathbb{Z}_{125}$.
2. $\mathbb{Z}_{72}$.
3. $\mathbb{Z}_{88}$.
4. $\mathbb{Z}_{1000}$.

Ejercicio 4 Determina si la igualdad $a = b$ es cierta en los siguientes casos:

1. $a = 9^{(55^9)}$ y $b = 7^{(70^{55})}$, en el anillo $\mathbb{Z}_{21}$.
2. $a = 2^{(5^{70})}$ y $b = 5^{(70^2)}$, en el anillo $\mathbb{Z}_{21}$.
3. $a = 12^{(55^{70})}$ y $b = 10^{(70^{55})}$, en el anillo $\mathbb{Z}_{22}$.
4. $a = 5^{(5^{70})} \cdot 11^{(5^{70})}$ y $b = 10^{(70^{22})}$, en el anillo $\mathbb{Z}_{22}$.

Ejercicio 5 Determinar los inversos que se proponen (si existen)

1. $\overline{x^2 + x + 1}^{\,-1}$ en el anillo $\mathbb{Z}_3[x]/x^3 + 2x + 1$.
2. $\overline{x + 1}^{\,-1}$ en el anillo $\mathbb{R}[x]/x^3 - 2x - 3$.
3. $\overline{x^2 + x}^{\,-1}$ en el anillo $\mathbb{Z}_2[x]/x^2 + 1$.
4. $\overline{x^3 + x + 1}^{\,-1}$ en el anillo $\mathbb{Z}_2[x]/x^2 + x + 1$.

Ejercicio 5 Determinar los inversos que se proponen (si existen)

1. $\overline{1 + i}^{\,-1}$ en el anillo $\mathbb{Z}[i]/3 + 2i$.
2. $\overline{2 - \sqrt{2}}^{\,-1}$ en el anillo $\mathbb{Z}[\sqrt{2}]/3$.
3. $\overline{3 + 3i\sqrt{2}}^{\,-1}$ en el anillo $\mathbb{Z}[i\sqrt{2}]/4 - 2i\sqrt{2}$.
4. $\overline{1 + \sqrt{3}}^{\,-1}$ en el anillo $\mathbb{Z}[\sqrt{3}]/\sqrt{3}$.

Tema 6

Dominios de Factorización Única

Recordemos que un elemento p en un Dominio de Integridad A es *irreducible* si no es cero ni unidad y sus únicos divisores son los triviales, esto es, las unidades y sus asociados, esto es, si no se pueden factorizar como $p = ab$ donde ni a ni b son unidades.

Definición 6.0.1. *Un Dominio de Factorización Única (DFU) es un dominio de integridad A en el cual todo elemento no nulo ni unidad $a \in A$ se puede expresar como un producto*

$$a = p_1 \cdots p_s$$

donde cada p_i es irreducible, y tal factorización es "esencialmente única", en el sentido si $a = q_1 \cdots q_t$ es otra, con cada q_j irreducible, entonces $s = t$ y hay una permutación $\sigma : \{1, \ldots, s\} \cong \{1, \ldots, s\}$ tal que cada p_i y $q_{\sigma(i)}$ son asociados.

Ejemplo. Las factorizaciones de -6 en $\mathbb{Z}$, $(-2) \cdot 3 = (-3) \cdot 2 = 3 \cdot (-2)$ son esencialmente la misma.

Si dos elementos del anillo son asociados, tienen los mismos divisores y, por tanto, uno es irreducible si y solo si lo es el otro. En un DFU, A, siempre podemos seleccionar un "*conjunto P, representativo de todos los irreducibles*", en el sentido que: (1) Todo elemento de P es irreducible, (2) Todo irreducible es asociado con uno de P, y (3) dos elementos distintos de P no son asociados. Por ejemplo, si $A = \mathbb{Z}$, podemos tomar como P el conjunto de los irreducibles positivos, y si $A = K[x]$ con K un cuerpo, podemos tomar como P el conjunto de los irreducibles mónicos (de coeficiente líder 1). En tal caso, cada elemento $a \in A$, $a \neq 0$, admite una factorización esencialmente única de la forma

$$a = up_1^{e_1} \cdots p_r^{e_r} = u \prod_{i=1}^{r} p_i^{e_i}, \tag{6.1}$$

donde u es una unidad, $r \geq 0$ ($a = u$ si $r = 0$), cada $p_i \in P$, cada exponente $e_i \geq 1$ es un entero positivo, y $p_i \neq p_j$ si $i \neq j$. En efecto, si a no es una unidad y $a = q_1 \cdots q_s$ es cualquier factorización en irreducibles de a, tendremos cada $q_j = u_j p_j$, con $p_j \in P$, para cierta unidad u_j. Entonces, tomando $u = u_1 \cdots u_t$, tendremos $a = up_1 \cdots p_t$, con $p_j \in P$, y u una unidad. Finalmente, reordenando loos factores irreducibles y agrupando todos los que se repitan, obtenemos una tal expresión de a.

Para cada elemento del DFU $a \in A$, $a \neq 0$, cuya factorización sea la dada en (6.1), y cada irreducible $p \in P$, denotaremos por

$$e(p, a)$$

al exponente con que p aparece en la factorización de de a, acordando que $e(p, a) = 0$ si p no aparece en la factorización. Esto es, para cada $i = 1, \ldots, r$, $ep_i, a) = e_i$, y para cualquier $p \notin \{p_1, \ldots, p_r\}$, ponemos $e(p, a) = 0$. Puesto que en tal caso es $p^{e(p,a)} = 1$, podemos usar la expresión

$$a = u \prod_{p \in P} p^{e(p,a)},$$

donde en realidad solo intervienen un número finito de factores distintos de uno, para indicar la factorización en irreducibles del elemento. Esta es útil para observar que en todo DFU hay mcd y mcm de cualesquiera dos elementos

Lema 6.0.2. *(i) Para cualesquiera elementos no nulos $a, b \in A$, y $p \in P$, se verifica que*

$$e(p, ab) = e(p, a) + e(p, c).$$

(ii) Para cualesquiera elementos no nulos $a, c \in A$, se verifica que

$$a|c \Leftrightarrow e(p, a) \leq e(p, c), \quad \forall p \in P.$$

Demostración. Si $a|c$ será $c = ab$ para un cierto b, pero entonces

$$e(p, c) = e(p, a) + e(p, b) \geq e(p, a).$$

Recíprocamente, si $a = u \prod_{p \in P} p^{e(p,c)}$, $c = v \prod_{p \in P} p^{e(p,c)}$, y $e(p, a) \leq e(p, c)$, para todo $p \in P$, definiendo $b = u^{-1} v \prod_{p \in P} p^{e(p,c)-e(p,a)}$, claramente $ab = c$ y $a|c$. ■

Proposición 6.0.3. *En un DFU existen mcd y mcm de cualesquiera elementos. Para $a, b \neq 0$, se tiene que*

$$mcd(a, b) = \prod_{p \in P} p^{min\{e(p,a), e(p,b)\}}, \qquad mcm(a, b) = \prod_{p \in P} p^{max\{e(p,a), e(p,b)\}}.$$

Demostración. Para cualquier $c \neq 0$, se tiene que $c|a$ y $c|b$ si y solo si, para todo $p \in P$, $e(p, c) \leq e(p, a)$ y $e(p, c) \leq e(p, a)$; esto es, si y solo si $e(p, c) \leq min\{e(p, b), e(p, b)$. Entonces $c|a$ y $c|b$ si y solo si $c| \prod_{p \in P} p^{min\{e(p,a), e(p,b)\}}$. ■

6.1 Caracterización de DFU

Definición 6.1.1. *Sea A un DI. Un elemento $p \in A$, no nulo ni unidad, se dice que es "primo" si verifica la siguiente propiedad*

$$p|ab \Rightarrow p|a \vee p|b.$$

En otras palabras, si p no divide a dos elementos, entonces tampoco divide a su producto.

Proposición 6.1.2.
(i) En cualquier DI, todo primo es irreducible.
(ii) En un DFU, un elemento es primo si y solo si es irreducible.

Demostración.

(*i*) Sea p es primo. Veamos que sus unicos divisores son los triviales. Supongamos que a es un divisor de p, y que no es asociado. Entonces p no divide a a. Como existirá un b tal que $p = ab$, y p es primo, será $p|a$ o $p|b$. Necesariamente entonces $p|b$. Pero $b|p$ y p y b serán asociados. Digamos que $p = ub$, con u una unidad. Entonces, $ub = ab$, implica que $a = u$, y a es unidad.

(*ii*) Sea p un irreducible en un DFU, que podemos suponer en P, y supongamos que $p|ab$. Entonces $1 = e(p,p) \leq e(p,ab) = e(p,a) + e(p,b)$. Necesariamente entonces $e(p,a) \geq 1$ o $e(p,b) \geq 1$. Luego $p|a$ o $p|b$. ■

Teorema 6.1.3. *Sea A un DI. Son equivalentes,*

(1) *A es un DFU.*

(2) $\begin{cases} \bullet \text{ todo elemento no nulo ni unidad es producto de irreducibles.} \\ \bullet \text{ existe mcd de todo par de elementos.} \end{cases}$

(3) $\begin{cases} \bullet \text{ todo elemento no nulo ni unidad es producto de irreducibles.} \\ \bullet \text{ todo irreducible es primo.} \end{cases}$

Demostración. La implicación (1) $\Rightarrow$ (2) es clara. Para ver que (2) $\Rightarrow$ (3), sea p un irreducible y supongamos que no divide ni a a ni a b. Entonces $(p,a) = 1 = (p,b)$. Entonces $b = b1 = b(p,a) = (pb, ab)$ y

$$1 = (p,b) = (p,(pb,ab)) = ((p,pb),ab) = (p(1,b),ab) = (p,ab),$$

de donde concluimos que p no divide a ab. Así que p es primo.

Veamos ahora que (3) $\Rightarrow$ (1), o sea la unicidad de las factorizaciones: Supongamos $p_1 \cdots p_r = q_1 \cdots q_s$, con los p_i y los q_j irreducibles, es decir primos en este caso. Hacemos inducción sobre $r \geq 1$. Si $r = 1$, tenemos que $p_1 = q_1 \cdots q_s$. Como p_1 es irreducible y los q_j no son unidades, ha de ser $m = 1$ y $q_1 = p_1$. Supongamos ahora $r > 1$ y damos por válido la unicidad de las factorizaciones en irreducibles donde una de ellas tiene menos de r factores irreducibles. Como $p_r|q_1 \cdots q_s$, y p_r es primo, ha de existir un j con $p_r|1q_j$. Pero p_r no tiene divisores propios, luego p_r y q_j han de ser asociados. Renumerando si es necesario, podemos suponer que $q_s = up_r$ para una cierta unidad u. Nos queda entonces

$$p_1 \cdots p_{r-1} = q_1 \cdots q_{s-2}(uq_{s-1}).$$

Entonces, por hipótesis de inducción $s = r$ y, salvo renumeración, cada p_i es asociado con el correspondiente q_i. □.

6.2 Todo DE es un DFU

Ya sabemos que en todo DE hay mcd de cualquier par de elementos. Bastará probar que en un DE, digamos A, todo elemento no nulo ni unidad factoriza en producto de irreducibles. Para ello, primero observamos: *Si a es un divisor propio de b, entonces $\rho(a) < \rho(b)$.* Si fuese $\rho(a) \geq \rho(b)$, entonces $\rho(a - bq) < \rho(b) \leq \rho(a)$ para algún $q \in A$; pero $b = ac$ para algún $c \in A$ y, sustituyendo, tenemos que $\rho(a - acq) < \rho(a)$. Pero $\rho(a - acq) = \rho(a(1 - cq)) \geq \rho(a)$, lo que es una contradicción.

Veamos todo elemento no nulo ni unidad factoriza en producto de irreducibles. Supongamos, por el contrario que eso es falso, esto es, que hay elementos, que son cero ni unidad, que no factorizan en producto de irreducibles, y hagamos la siguiente observación:

Si a es un tal elemento, hay un divisor propio a' de a que tampoco admite una tal factorización.

En efecto, ese a no sería un irreducible y tendría una factorización como $a = bc$, con b y c divisores propios de a. Si ambos se pudieran factorizar como producto de irreducibles, $b = p_1 \cdots p_r$ y $b = q_1 \cdots q_s$, es claro que el propio a se factorizaría $a = p_1 \cdots p_r q_1 \cdots q_s$. Luego al menos uno de ellos no tiene una tal factorización. Sea a' ese elemento. Formemos la sucesión de elementos $a_1, a_2, \ldots, a_n, \ldots$, por la regla $a_1 = a$, y $a_{n+1} = a'_n$. Por construcción cada $a_{n+1} | a_n$ y es un divisor propio. Entonces $\rho(a_n) > rho(a_{n+1})$ y la cadena de naturales $\rho(a) = \rho(a_1) > \rho(a_2) > \cdots > \rho(a_n) > \cdots$, es infinita! □

Como corolario inmediato, tenemos que

Teorema 6.2.1 (Teorema fundamental de la Aritmética)**.**
El anillo de los enteros $\mathbb{Z}$ es un Dominio de Factorización Única.

Pero también los anillos de polinomios $K[x]$, con K un cuerpo, son DFU. También el anillo de los enteros de Gauss $\mathbb{Z}[i]$, o $\mathbb{Z}[\sqrt{2}]$, etc, son DFU.

El siguiente teorema es históricamente muy relevante

Teorema 6.2.2 (Euclides)**.** *En $\mathbb{Z}$ hay infinitos primos positivos.*

Demostración. Supongamos, por el contrario, que solo hubiera un número finito de ellos, digamos $p_1, \ldots, p_r$. En número $m = 1 + p_1 \cdots p_r$ no es cero ni unidad, tendrá una factorización en producto de primos. Habrá entonces un p_i de los anteriores que divida a m. Pero entonces, ese p_i dividirá a $m - p_1 \cdots p_r = 1$, lo que es imposible. ■

6.3 Irreducibles y primos en $\mathbb{Z}[\sqrt{n}]$

Lema 6.3.1. *Si α es un divisor propio de β en $\mathbb{Z}[\sqrt{n}]$, entonces $N(\alpha)$ es un divisor propio de $\mathbb{N}(\beta)$ en $\mathbb{Z}$.*

Demostración. Será $N(\alpha) \neq \pm 1$, y existe un α' con $N(\alpha') \neq \pm 1$ tal que $\beta = \alpha\alpha'$ con $N(\alpha') \neq \pm 1$. Pero entonces la igualdad $N(\beta) = N(\alpha)N(\alpha')$ nos dice que $N(\alpha)$ es un divisor propio de $\mathbb{N}(\beta)$ en $\mathbb{Z}$. ■

Proposición 6.3.2. *Sea $\alpha \in \mathbb{Z}[\sqrt{n}]$.*
(1) *Si $N(\alpha) = \pm p$, con p primo de $\mathbb{Z}$, entonces α es irreducible.*
(2) *Si α es primo en $\mathbb{Z}[\sqrt{n}]$, entonces $N(\alpha) \in \{\pm p, \pm p^2\}$, con $p \geq 2$ un primo de $\mathbb{Z}$. Además, si $N(\alpha) = \pm p^2$, entonces α y p son asociados en $\mathbb{Z}[\sqrt{n}]$.*

Demostración.
(1) Por el Lema 6.3.1 anterior, si α tuviera divisores propios, $N(\alpha) = \pm p$ los tendría. Luego α es irreducible.

(2) Supongamos α es primo. Observemos primero que hay un p primo de $\mathbb{Z}$ tal que $p = \alpha\beta$ para algún $\beta \in \mathbb{Z}[\sqrt{n}]$: En efecto, si $N(\alpha) = p_1 \cdot p_r$ con p_i primos de $\mathbb{Z}$, como $\mathbb{N}(\alpha) = \alpha\overline{\alpha}$, tenemos que $\alpha | p_1 \cdots p_r$, y como α es primo, será α / p_i para algún i, así que $p_i = \alpha\beta$ para algún β.

De la igualdad $p = \alpha\beta$, deducimos que $p^2 = N(\alpha)N(\beta)$. Entonces, $N(\alpha) | N(p) = p^2$ en $\mathbb{Z}$. Luego $N(\alpha) \in \{\pm p, \pm p^2\}$ (no puede ser ± 1 pues α no es unidad). Además, si $N(\alpha) = \pm p^2$, tendremos que $p^2 = N(\alpha)N(\beta) = \pm p^2 N(\beta)$, de donde $N(\beta) = \pm 1$, y β es unidad. Como $p = \alpha\beta$, p y α son asociados. ■

Nota. Si $N(\alpha) = p^2$, con p un primo de $\mathbb{Z}$, no tiene por qué ser α irreducible (ni primo, entonces). Por ejemplo, en $\mathbb{Z}[i]$, $N(2) = 2^2$, pero no es irreducible: $2 = (1+i)(1-i)$.

EJEMPLOS.

1. *Factorizar $11 + 7i$ en producto de irreducibles (= primos) en el anillo $\mathbb{Z}[i]$.*

Como $\mathbb{Z}[i]$ es un DE, es un DFU y tal factorización existe. Observemos que su norma es $N(11+7i) = 11^2+7^2 = 170 = 2\cdot 5\cdot 17$. Claramente $11+7i$ no es irreducible, pues su norma no es un primo, ni el cuadrado de un primo de $\mathbb{Z}$. Si α es un divisor primo de $11+7i$, su norma será un divisor propio de 170 y será un primo o el cuadrado de un primo de $\mathbb{Z}$. Pero ningún primo al cuadrado de $\mathbb{Z}$ divide a 170, luego la norma de ese divisor primo habrá de ser 2, 5 o 17. Veamos que tiene un divisor primo de norma 2: Enteros de Gauss de norma 2, son los $\alpha = a+bi$ tal que $a^2+b^2 = 2$, o sea $a = \pm 1 \wedge b \pm 1$. Esto es, $\alpha = 1+i$ y sus asociados $(-1+i, -1-i, 1-i)$. Como

$$\frac{11+7i}{1+i} = \frac{(11+7i)(1-i)}{2} = \frac{11-11i+7i+7}{2} = \frac{18-4i}{2} = 9-2i \in \mathbb{Z}[i],$$

obtenemos que $1+i|11+7i$ y, de hecho, $11+7i = (1+i)(9-2i)$, donde $1+i$ es irreducible al ser de norma 2.

Nos centramos ahora en $9-2i$.

Como $N(9-2i) = 81+4 = 85 = 5\cdot 17$, este no es irreducible. Busquemos divisores de norma 5:

Si $N(a+bi) = 5$, será porque $a^2+b^2 = 5 \Leftrightarrow (a = \pm 2 \wedge b = \pm 1) \vee (a = \pm 1 \wedge b = \pm 2)$. Esto es, $2+i$ y sus asociados $(-2-2i, -1+2i, 1-2i)$ y $1+2i$ y sus asociados $(-1-2i, -2+i, 2-i)$. Veamos si $2+i/9-2i$:

$$\frac{9-2i}{2+i} = \frac{(9-2i)(2-i)}{5} = \frac{18-9i-4i-2}{5} = \frac{16-13i}{5} \notin \mathbb{Z}[i].$$

Veamos si $1+2i|9-2i$:

$$\frac{9-2i}{1+2i} = \frac{(9-2i)(1-2i)}{5} = \frac{9-18i-2i-4}{5} = \frac{5-20i}{5} = 1-4i \in \mathbb{Z}[i].$$

así que $1+2i|9-2i$ y, $9-2i = (1+2i)(1-4i)$, donde $1+2i$ es primo al ser de norma 5. Pero $(1-4i$ también, al ser de norma $1+16 = 17$ primo de $\mathbb{Z}$.

Conclusión, la factorización pedida es $11+7i = (1+i)(1+2i)(1-4i)$. □

2. *Calcular $(2i, 11+7i)$ y $[2i, 11+7i]$ en $\mathbb{Z}[i]$.*

Como $2i$ es asociado con 2, podemos sustituir $2i$ por 2 en la cuestión. Buscamos la factorización en primos de $2i$ en $\mathbb{Z}[i]$: Como $N(2i) = 4 = 2^2$, Bien $2i$ es irreducible o tiene un factor irreducible de norma 2. Antes hemos visto que los enteros de Gauss de norma 2 son $1+i$ y sus asociados. Luego 2 es irreducible, o es divisible por $1+i$:

$$\frac{2i}{1+i} = \frac{2i(1-i)}{2} = \frac{2i+2}{2} = 1+i \in \mathbb{Z}[i].$$

así que $2 = (1+i)^2$ es la factorización del 2 en irreducibles en $\mathbb{Z}[i]$. Entonces,

$$(2i, 11+7i) = ((1+i)^2, (1+i)(1+2i)(1-4i)) = 1+i.$$

$[2i, 11+7i] = [(1+i)^2, (1+i)(1+2i)(1-4i)] = (1+i)^2(1+2i)(1-4i) = 2i(9-2i) = 4+18i.$ □

3. *Factorizar* 180 *en producto de irreducibles (= primos) en el anillo* $\mathbb{Z}[\sqrt{-2}]$.

En $\mathbb{Z}$ tenemos que $180 = 2 \cdot 90 = 2^2 \cdot 45 = 2^2 \cdot 3^3 \cdot 5$. Busquemos las factorizaciones en $\mathbb{Z}[\sqrt{-2}]$ de 2, 3 y 5.

Para factorizar 2, como $N(2) = 4$, bien 2 es irreducible o es divisible por un irreducible de norma 2: $N(a + b\sqrt{2-}) = a^2 + 2b^2 = 2 \Leftrightarrow b = \pm 1 \wedge a = 0$. El único irreducible de norma 2 es $\sqrt{-2}$, y su asociado $-\sqrt{-2}$:

$$\frac{2}{\sqrt{-2}} = \frac{2 \cdot (-\sqrt{-2})}{2} = -\sqrt{-2},$$

Luego $2 = \sqrt{-2}(-\sqrt{-2}) = -(\sqrt{-2})^2$ es la factorización de 2 en producto de irreducibles.

Para factorizar 3, como $N(3) = 9$, bien 3 es irreducible o es divisible por un irreducible de norma 3: $N(a + b\sqrt{2-}) = a^2 + 2b^2 = 3 \Leftrightarrow b = \pm 1 \wedge a = \pm 1$. Los únicos irreducibles de norma 3 son $1 + \sqrt{-2}$, $1 - \sqrt{-2}$, y sus asociados $-1 - \sqrt{-2}$ y $-1 + \sqrt{-2}$:

$$\frac{3}{1 + \sqrt{-2}} = \frac{3 \cdot (1 - \sqrt{-2})}{3} = 1 - \sqrt{-2},$$

Luego $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$ es la factorización de 3 en producto de irreducibles.

Para factorizar 5, como $N(5) = 5^2$, bien 5 es irreducible o es divisible por un irreducible de norma 5: Pero en $\mathbb{Z}[\sqrt{-2}]$ no existen elementos de norma 5, pues $N(a+b\sqrt{2-}) = a^2+2b^2 = 5$ y vemos que no existen tales a y b. Luego 5 es irreducible en $\mathbb{Z}[\sqrt{-2}]$.

Conclusión: La factorización buscada es

$$180 = (-5)(\sqrt{-2})^2(1 + \sqrt{-2})^3(1 - \sqrt{-2})^3,$$

salvo orden y asociados. □

4. *En* $\mathbb{Z}[\sqrt{-5}]$ *hay irreducibles que no son primos.*

Ya vimos que en este anillo no hay mcd de cualesquiera par de elementos. Por tanto no es un DFU. Veamos ahora que hay irreducibles que no son primos y como hay factorizaciones en irreducibles que no son equivalentes. Consideremos $1 + \sqrt{-5}$, su norma es $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 1 + 5 = 6 = 2 \cdot 3$. Si $1 + \sqrt{-5}$ no fuese irreducible, tendría divisores de norma 2 o 3. Pero no hay elementos en este anillo de tales normas (la ecuaciónes $a^2 + 5b^2 = 2$ y $a^2+5b^2 = 3$, no tienen soluciones en $\mathbb{Z}$). Luego $1+\sqrt{-5}$ es irreducible y, por la misma razón, $1 - \sqrt{-5}$ también lo es, así como lo son 2 y 3 (cuyas normas son 4 y 9, respectivamente).

Ahora, 2 no es primo, pues $2|6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ y, sin embargo, 2 no divide a $(1 + \sqrt{-5})$ ni a $(1 - \sqrt{-5})$. Si dividiese a alguno de ellos, tomando normas, 4 dividiría a 6, lo que no ocurre. Por la mismas razones 3, $1 + \sqrt{-5}$ y $1 + \sqrt{-5}$ son todos irreducibles pero no primos.

Finalmente, destaquemos que las dos factorizaciones del 6 en producto de irreducibles

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$$

son esencialmente diferentes, pues los irreducibles que intervienen no son asociados. □

6.4 Factorización única en anillos de polinomios

Conocemos que, si K es un cuerpo, entonces $K[x]$ es un DE y, por tanto, un DFU. Pero hay anillos de polinomios interesantes, por ejemplo $\mathbb{Z}[x]$, que son DFU aun no siendo Dominios Euclídeos.

Vamos, con generalidad, a estudiar el carácter DFU de un anillo $A[x]$ donde el anillo de coeficientes A es un DFU. En lo que sigue, denotaremos por $K = \mathbb{Q}(A)$ al cuerpo de fracciones de A, y tendremos muy en cuenta que $A[x] \subseteq K[x]$ es un subanillo.

Para demostrar que $A[x]$ es un DFU, utilizaremos que $K[x]$ lo es, y necesitaremos relacionar los irreducibles de estos anillos. Una primera observación al respecto concierne a los irreducibles de grado cero de $A[x]$. Notemos que en $K[x]$ no hay irreducibles de grado cero (pues todos son unidades).

Lema 6.4.1. *Un elemento $a \in A$ es irreducible en $A[x]$ si y solo si lo es en A.*

Demostración. Si a es irreducible en A y $a = fg$ en $A[x]$, necesariamente f y g serían de grado cero. Esto es $f = b \in A$ y $g = c \in A$. Entonces $a = bc$ en A y b o c son unidades de A, o sea f o g unidades de $A[x]$. Luego a es irreducible en $A[x]$. Reciprocamente, si a es irreducible en $A[x]$, y $a = bc$ en A, esa misma factorización es válida en $A[x]$ y por tanto b o c es una unidad de $A[x]$, o sea de A. ■

Para polinomios de grado ≥ 1, el siguiente concepto es muy útil.

Definición 6.4.2. *Se define el "contenido" de un polinomio $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$, $n \geq 1$, como el mcd de sus coeficientes, esto es*

$$c(f) = (a_0, \ldots, a_n).$$

Decimos que f es "primitivo" si $c(f) = 1$.

Lema 6.4.3.

(i) Para cualquier $a \in A$ y $f \in A[x]$, de grado ≥ 1, se verifica que $c(af) = a\,c(f)$.

(ii) Todo polinomio $g \in A[x]$, de grado ≥ 1, se expresa de forma única como $g = af$, donde $a = c(g) \in A$ y $f \in A[x]$ es primitivo.

(iii) Todo polinomio no nulo $\phi \in K[x]$, de grado ≥ 1, se expresa de forma única como $\phi = \frac{a}{b}f$, donde $\frac{a}{b} \in K$ y $f \in A[x]$ es primitivo.

Demostración.

(i) $(aa_0, \ldots, aa_n) = a(a_0, \ldots, a_n)$.

(ii) Supongamos que $f = a_0 + a_1x + \cdots + a_nx^n$ y sea $a = c(f)$. Pongamos $a_i = c\,a_i'$ y $g = a_0' + a_1'x + \cdots + a_n'x^n$. Tenemos $f = ag$ y, como $a = c(ag) = a\,c(g)$, necesariamente $c(g) = 1$ (pues $a \neq 0$). Para la unicidad, si $ag = bh$, con g, h ambos primitivos, tomando contenidos tendríamos $a\,c(g) = b\,c(h)$, o sea que $a = b$, de donde también $g = h$.

(iii) Supongamos que $\phi = \sum_{i\geq 0}^{n} \frac{a_i}{b_i}x^i$. Si $b = \prod_{i\geq 0} b_i$, entonces $b\phi = \sum_{i\geq 0}^{n} \frac{ba_i}{b_i}x^i$. Claramente $\frac{ba_i}{b_i} = c_i \in A$, así que $b\phi \in A[x]$. Pongamos $b\phi = af$, con f primitivo. Entonces $\phi = \frac{a}{b}f$ en las condiciones anunciadas. Para la unicidad, supongamos que $\phi = \frac{a'}{b'}f'$, con $f' \in A[x]$ primitivo. Entonces de la igualdad $ab'f = a'bf'$, resulta que $ab' = a'b$, o sea que $\frac{a}{b} = \frac{a'}{b'}$. Claramente entonces también $f = f'$. ■

Teorema 6.4.4 (Lema de Gauss)**.** *El producto de dos polinomios primitivos es primitivo.*

Demostración. Sean $f = \sum_{i\geq 0} a_i x^i$ y $g = \sum_{j\geq 0} a_j x^j$, ambos primitivos. Pongamos $fg = \sum_{k\geq 0} c_k x^k$, donde cada $c_k = \sum_{i+j=k} a_i b_j$, y supongamos que fg no es primitivo. Como A es un DFU, existirá algún irreducible $p \in A$ tal que $p|c(fg)$, esto es, tal que $p|c_k$ para todo k. Como f y g son primitivos, ese irreducible p no puede dividir a todos los a_i ni a todos los b_j. Sear a_r el primer coeficiente de f que no es divisible por p y b_s el primero de g que no es divisible por p. Como p es primo, entonces p no divide a $a_r b_s$. Pero $p|c_{r+s}$ y tenemos que

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j = \sum_{i<r} a_i b_{r+s-i} + a_r b_s + \sum_{i>r} a_i b_{r+s-i}.$$

Para todo $i < r$ tenemos que $p|a_i$ y para todo $i > r$ tenemos que $p|b_{r+s-i}$ (pues $r + s - i < r + s - r = s$). Entonces p divide a todos los sumandos del primer y del segundo sumatorio. Desde hay, se concluye que $p|c_{r+s}$, lo que es una contradicción. ■

Corolario 6.4.5. *Para todos $f, g \in A[x]$, , de grado ≥ 1, se verifica que $c(fg) = c(f)\, c(g)$.*

Demostración. Como $fg = c(f)c(g)f'g'$, será $c(fg) = c(f)c(g)c(f'g') = c(f)c(g)$. ■

Teorema 6.4.6. *Sea $\phi \in K[x]$ un polinomio, de grado ≥ 1. Supongamos $\phi = \frac{a}{b} f$, donde $f \in A[x]$ es primitivo. Son equivalentes*

1. *ϕ es irreducible en $K[x]$.*
2. *f es irreducible en $K[x]$.*
3. *f es irreducible en $A[x]$.*

Demostración.

Puesto que ϕ y f son asociados en $K[x]$, uno será irreducible si y solo si lo es el otro, así que (1) $\Leftrightarrow$ (2).

(2) $\Rightarrow$ (3): Supongamos que f no es irreducible en $A[x]$. Será $f = f_1 f_2$, con $f_1, f_2 \in A[x]$ no unidades de A. Notemos que ni f_1 ni f_2 son de grado cero (pues si, por ejemplo, $f_1 = a_1 \in A$, entonces $1 = c(f) = a_1 c(f_2)$ y $f_1 = a_1 \in U(A)$). Así que $gr(f_1), gr(f_2) \geq 1$. Pero entonces ni f_1 ni f_2 son unidades en $K[x]$ y la propia igualdad $f = f_1 f_2$ nos dice que f no es irreducible en $K[x]$.

(3) $\Rightarrow$ (2) Supongamos que f no es irreducible en $K[x]$. Será $f = \phi_1\phi_2$, con $\phi_1, \phi_2 \in K[x]$, ambos de grado ≥ 1. Pongamos $\phi_i = \frac{a_i}{b_i} f_i$, $i = 1, 2$, con $f_i \in A[x]$ primitivo. Entonces, la igualdad $f = \frac{a_1 a_2}{b_1 b_2} f_1 f_2$, donde f y $f_1 f_2$ son primitivos, nos lleva a que $\frac{a_1 a_2}{b_1 b_2} = 1$ y $f = f_1 f_2$, donde tanto f_1 como f_2 son de grado ≥ 1. Esto niega que f es irreducible en $A[x]$. ■

Corolario 6.4.7. *Un polinomio $f \in A[x]$ con $gr(f) \geq 1$ es irreducible si y solo si es primitivo e irreducible en $K[x]$.*

Demostración. Si f es irreducible en $A[x]$, necesariamente es primitivo, pues en otro caso $f = c(f)f'$ es una factorización de f donde ninguno de los factores es una unidad. Entonces f es irreducible en $K[x]$ por el teorema 6.4.6 anterior. El recíproco también lo da el teorema 6.4.6 anterior. ■

Teorema 6.4.8 (Teorema de Gauss)**.** *Si A es un DFU, entonces $A[x]$ es un DFU.*

Demostración. Sea $f \in A[x]$, no nulo ni unidad. Probamos primero que f puede factorizarse en producto de irreducibles de $A[x]$. Si f es de grado cero, $f = a$, como A es un DFU, será $a = p_1 \cdots p_r$ con p_i irreducibles de A, y por tanto también irreducibles de $A[x]$. Si f es de

grado ≥ 1, pongamos $f = ag$, con $a = c(f) \in A$ y $g \in A[x]$ primitivo. Si $a \neq 1$, factorizamos $a = p_1 \cdots p_r$ en A, con p_i irreducibles de A, y por tanto también de $A[x]$. Factorizamos ahora g en $k[x]$: $g = \phi_1 \cdots \phi_s$, con los ϕ_j irreducibles de $K[x]$ (en particular todos de grado ≥ 1). Expresamos estos en la forma $\phi_j = \frac{a_j}{b_j} f_j$, con los $f_j \in A[x]$ primitivos. Estos son entonces irreducibles an $A[x]$. Ademas, la igualdad

$$g = \frac{a_1 \cdots a_s}{b_1 \cdots b_s} f_1 \cdots f_s$$

implica que $\frac{a_1 \cdots a_s}{b_1 \cdots b_s} = 1$ y que $g = f_1 \cdots f_s$. Luego

$$f = p_1 \cdots p_r f_1 \cdots f_s$$

es una factorización de f en producto de irreducibles de $A[x]$.

Veamos ahora que en $A[x]$ todo irreducible es primo. Si p es un irreducible de grado cero de $A[x]$, o sea un irreducible de A, y $p|fg$, para $f, g \in A[x]$, será $ph = fg$ para un cierto $h \in A[x]$. Pero entonces $p\,c(h) = c(f)\,c(g)$ en A, y como p es primo en A, será $p|c(f)$ o $p|c(g)$. Entonces $p|f$ o $p|g$, respectivamente.

Supongamos ahora que $f \in A[x]$ es un irreducible de grado ≥ 1, por tanto primitivo y primo en $K[x]$, tal que $f|gh$ en $A[x]$. Puesto que entonces $f|gh$ también en $K[x]$, será $f|h$ o $f|h$ en $K[x]$. Supongamos es $f\phi = g$ para un cierto $\phi \in K[x]$. Pongamos $\phi = \frac{a}{b} f'$ con $f' \in A[x]$ primitivo. Entonces $\frac{a}{b} ff' = g$, de donde $aff' = bg$ y $a = bc(g)$ (pues f y f' son primitivos). Pero entonces $\frac{a}{b} = c(g)$ y $f(c(g)f') = g$, luego $f|g$ en $A[x]$. ■

6.4.1 Criterios básicos de irreducibilidad de polinomios

Nos ocuparemos aquí de mostrar algunos criterios básicos para el reconocimiento de polinomios irreducibles, con interés fundamentalmente en polinomios con coeficientes enteros y racionales. Los casos, también muy interesantes, de polinomios reales y complejos no podemos discutirlos aquí (necesitan conocimientos más elevados), pero si podremos enunciar lo que resulta en estos casos.

Comenzamos con unas observaciones generales sobre polinomios en $K[x]$, con K un cuerpo.

• *En $K[x]$ todo polinomio es asociado con uno "*mónico*"*, esto es, con coeficiente lider 1: En efecto, si $\phi = \alpha_0 + \alpha_1 x + \cdots \alpha_n x^n$ con $\alpha_n \neq 0$, entonces ϕ es asociado con $\psi = \alpha_n^{-1}\phi$, cuyo coeficiente lider es 1. Además, dos polinomios mónicos son asociados si y solo si son iguales. Por tanto, para conocer los irreducibles de $K[x]$ (salvo asociados) basta conocer los irreducibles mónicos.

• *En $K[x]$ no hay irreducibles de grado* 0, pues todos estos son unidades.

Para polinomios de grado 1, tenemos que

Proposición 6.4.9. *Todo polinomio de grado* 1 *en $K[x]$ es irreducible.*

Demostración. Si $\phi \in K[x]$ es de grado 1 y $\phi = \phi_1\phi_2$, tendríamos $1 = gr(\phi_1) + gr(\phi_2)$, lo que obliga a que uno de ellos tenga grado 0, o sea se trata de una unidad de $K[x]$. ■

Así, los irreducibles mónicos de grado 1 en $K[x]$ son todos los polinomios $x + \alpha$, con $\alpha \in K$. Así, por ejemplo, cuando el cuerpo de coeficientes es un $\mathbb{Z}_p$, los irreducibles mónicos de grado 1 son x, $x + 1$, ..., $x + p - 1$. Para polinomios con coeficientes complejos, más adelante se os probara lo siguiente:

Teorema 6.4.10 (Teorema fundamental del Álgebra (Gauss)). *En $\mathbb{C}[x]$ los únicos polinomios irreducibles son los de grado 1.*

El siguiente "*Criterio de la raíz*" es muy útil para saber si uno de los irreducibles mónicos de grado 1 aparece o no en la factorización de un polinomio de $K[x]$.

Proposición 6.4.11 (Ruffini). *Dado $\phi \in K[x]$ y $\alpha \in K$, se verifica que $(x-\alpha)|\phi \Leftrightarrow \phi(\alpha) = 0$.*

Demostración. $\phi = (x-\alpha)\psi$ en $K[x]$, entonces $\phi(\alpha) = (\alpha-\alpha)\psi(\alpha) = 0\psi(\alpha) = 0$. Recíprocamente, Si $\phi(\alpha) = 0$, al dividir ϕ entre $x-\alpha$, será $\phi = (x-\alpha)\psi(x) + \beta$, para un cierto $\beta \in K$. Pero entonces $0 = \phi(\alpha) = 0\psi(\alpha) + \beta = \beta$ y $\phi = (x-\alpha)\psi(x)$. Por tanto $(x-\alpha)|\phi$. ■

Corolario 6.4.12. *Si $\phi \in K[x]$ tiene grado 2 o 3, entonces ϕ es irreducible si y solo si no tiene raíces K.*

Demostración. Si ϕ tiene una raíz α, entonces $x-\alpha/\phi$ y ϕ no es irreducible. Recíprocamente, si ϕ no es irreducible, sería $\phi = \phi_1\phi_2$ donde ninguno de estos es de grado cero. Pero entonces uno es de grado uno y, asociado a uno de la forma $x-\alpha$. Luego $x-\alpha|\phi$ y $\phi(\alpha) = 0$. ■

Para polinomios con coeficientes reales, utilizando lo anterior, más adelante, se os probará lo siguiente.

Teorema 6.4.13. *En $\mathbb{R}[x]$ los únicos polinomios irreducibles son los de grado 1 y los de grado 2 de la forma ax^2+bx+c tales que $b^2-4ac<0$. Por tanto, los mónicos irreducibles de $\mathbb{R}[x]$ son los $x+a$, y x^2+bx+c con $a,b,c \in \mathbb{R}$ y $b^2-4c<0$.*

Con el anterior criterio de Ruffini, por ejemplo, podemos incluso listar todos los irreducibles mónicos de grado 2 en los primeros $\mathbb{Z}_p[x]$:

- En $\mathbb{Z}_2[x]$: x^2+x+1.

- En $\mathbb{Z}_3[x]$: x^2+1, x^2+x+2, x^2+2x+2.

- En $\mathbb{Z}_5[x]$: x^2+2, x^2+3, x^2+x+1, x^2+x+2, x^2+2x+3, x^2+2x+4, x^2+3x+3, x^2+3x+4, x^2+4x+1, x^2+4x+2.

Y de grado 3:

- En $\mathbb{Z}_2[x]$: x^3+x+1, x^3+x^2+1.

- En $\mathbb{Z}_3[x]$: x^3+2x+1, x^3+2x+2, x^3+x^2+2, x^3+2x^2+1, x^3+x^2+x+2, x^3+x^2+2x+1, x^3+2x^2+x+1, x^3+2x^2+2x+2.

Con esa información, ya podemos factorizar completamente polinomios en $\mathbb{Z}_2[x]$ y en $\mathbb{Z}_3[x]$ de hasta grado 7, y en $\mathbb{Z}_5[x]$ de hasta grado 5.

EJEMPLOS. 1. *Factorizar $f = x^4+x^3+x^2+x+1$ en $\mathbb{Z}_2[x]$.*

Vemos que ni 0 ni 1 son raíces, por tanto f no tiene factores irreducibles de grado 1. Pero entonces tampoco los tiene de grado 3. Si tuviese un factor irreducible de grado 2, este sería x^2+x+1. Pero al hacer la división, resulta que $f = (x^2+x+1)x^2 + (x+1)$ y x^2+x+1 no divide a f. Luego f es irreducible.

2. *Factorizar $f = x^5+x^4+1$ en $\mathbb{Z}_2[x]$.*

Vemos que ni 0 ni 1 son raíces, por tanto f no tiene factores irreducibles de grado 1, y entonces tampoco los tiene de grado 4. Si tuviese un factor irreducible de grado 2, este sería x^2+1, x^2+x+2 o x^2+2x+2. Dividiendo,

resulta que $f = (x^2+x+2)(x^3+x)+x+1$, $f = (x^2+1)(x^3+x^2+2x)+x+1$, y $f = (x^2+2x+2)(x^3+2x^2)+2$. Luego f es irreducible.

3. *Factorizar* $f = x^5+x^4+x^2+1$ *en* $\mathbb{Z}_3[x]$.

Vemos que $f(0) = 1$, $f(1) = 1$ y $f(2) = f(-1) = -1+1+1+1 = 2$, por tanto f no tiene factores irreducibles de grado 1, y entonces tampoco los tiene de grado 4. Si tuviese un factor irreducible de grado 2, estos podrían ser x^2+1, x^2+x-1 o x^2-x-1, ninguno de los tres lo divide y por tanto el polinomio es irreducible.

Nos ocupamos en lo que sigue del caso específico de polinomios con coeficientes enteros y racionales, esto es, de polinomios en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$, que estudiamos simultáneamente. Recordar que

• *Los irreducibles de grado 0 en* $\mathbb{Z}[x]$ *son los propios irreducibles de* $\mathbb{Z}$, esto es, salvo signo, $2, 3, 5, 7, \ldots$, mientras que en $\mathbb{Q}[x]$ no los hay.

• *Si un polinomio* $f \in \mathbb{Z}[x]$ *de grado* ≥ 1 *es irreducible en* $\mathbb{Z}[x]$*, entonces es primitivo.*

• *Si* f *es primitivo, entonces* f *es irreducible en* $\mathbb{Z}[x]$ *si y solo si lo es en* $\mathbb{Q}[x]$.

• *Todo polinomio de grado* ≥ 1*,* $\phi \in Q[x]$*, se escribe de forma única como* $\phi = \frac{a}{b}f$*, con* $\frac{a}{b} \in \mathbb{Q}$ *y* $f \in \mathbb{Z}[x]$ *primitivo.* Entonces ϕ y f son asociados en $\mathbb{Q}[x]$, por tanto que ϕ es irreducible en $\mathbb{Q}[x]$ si y solo si f lo es en $\mathbb{Z}[x]$. Esto nos permite estudiar la irreducibilidad de polinomios en $\mathbb{Q}[x]$ estudiando la de los polinomios en $\mathbb{Z}[x]$ que son primitivos.

Sabemos que todo polinomio de grado 1 es irreducible en $\mathbb{Q}[x]$, por tanto un polinomio $a+bx \in \mathbb{Z}[x]$, con $b \neq 0$, será irreducible en $\mathbb{Z}[x]$ si y solo si es primitivo, o sea que

• *Un polinomio* $a+bx \in \mathbb{Z}[x]$*, con* $b \neq 0$*, es irreducible en* $\mathbb{Z}[x]$ *si y solo si* $(a, b) = 1$.

Sabemos también que un polinomio en $\mathbb{Q}[x]$ de grado 2 o de grado 3 es irreducible si y solo si no tiene raíces en $\mathbb{Q}$, por tanto

• *Un polinomio de grado* 2 *o* 3 *en* $\mathbb{Z}[x]$ *es irreducible si y solo si es primitivo y no tiene raíces en* $\mathbb{Q}$.

El siguiente hecho es relevante para saber como factorizar un polinomio en $\mathbb{Z}[x]$ que tiene una raíz en $\mathbb{Q}$, y por tanto que no es irreducible.

• *Supongamos* $f \in \mathbb{Z}[x]$ *con* $f(\frac{a}{b}) = 0$*, donde* $(a, b) = 1$*. Entonces* $(bx-a)/f$ *en* $\mathbb{Z}[x]$, y el polinomio $g \in \mathbb{Z}[x]$ tal que $f = (bx-a)g$ se calcula simplemente como el cociente de dividir f entre $bx-a$ en $\mathbb{Q}[x]$.

En efecto, sabemos que $(x-\frac{a}{b})/f$ en $\mathbb{Q}[x]$. Sea ϕ el cociente de dividir f entre $(x-\frac{a}{b})$. Será $f = (x-\frac{a}{b})\phi$. Pongamos $\phi = \frac{c}{d}h$, con $h \in \mathbb{Z}[x]$ primitivo. Entonces $f = (x-\frac{a}{b})\frac{c}{d}h$, de donde $bdf = c(bx-a)h$ y $bd\, c(f) = c$. Luego d/c y concluimos que $\phi \in \mathbb{Z}[x]$. $\square$

La siguiente información, sobre las posible raíces en $\mathbb{Q}$ de un polinomio con coeficientes en $\mathbb{Z}$, es también muy útil.

• *Sea* $f = a_0+a_1x+\cdots a_nx^n \in \mathbb{Z}[x]$*, con* $a_n \neq 0$*. Si* $f(\frac{a}{b}) = 0$*, donde* $(a, b) = 1$*, entonces* a/a_0 *y* b/a_n *en* $\mathbb{Z}$.

En efecto, como tendremos una igualdad en $\mathbb{Z}[x]$ de la forma

$$a_0 + a_1x + \cdots + a_nx^n = (bx-a)(b_0 + b_1x + \cdots + b_{n-1}x^{n-1}),$$

la igualdad entre los correspondientes coeficientes de grado 0, nos dice que $a_0 = a(-b_0)$, y la de los coeficientes de grado n que $a_n = bb_{n-1}$. Por tanto a/a_0 y b/a_n. $\square$.

La observación anterior, tiene aplicaciones inmediatas interesantes. Por ejemplo:

1. *Todas las raíces en $\mathbb{Q}$ de un polinomio mónico $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ están en $\mathbb{Z}$. Por tanto, si este no tiene raíces en $\mathbb{Z}$, tampoco las tiene en $\mathbb{Q}$.*

2. *Si $n \in \mathbb{Z}$ no es un cuadrado en $\mathbb{Z}$, esto es, si $\sqrt{n} \notin \mathbb{Z}$ no es un entero, tampoco lo es en $\mathbb{Q}$, esto es $\sqrt{n} \notin \mathbb{Q}$, es un irracional.* (Ya que si $x^2 - n$ no tiene raíz en $\mathbb{Z}$ tampoco la tiene en $\mathbb{Q}$)

EJEMPLOS. 1. *Factorizar $f = 20x^4 - 10x^3 - 80x^2 + 80x - 20$ en $\mathbb{Z}[x]$.*

Claramente $c(f) = 10$. Entonces $f = 10g = 2 \cdot 5 \cdot g$, con $g = 2x^4 - x^3 - 8x^2 + 8x - 2$, que es primitivo. Sus posibles raíces en $\mathbb{Q}$ son ± 1, $\pm\frac{1}{2}$, y ± 2. Probando, vemos que $g(\frac{1}{2}) = 0$. Por tanto es seguro que $2x - 1/g$ en $\mathbb{Z}[x]$. Hacemos la divisón en $\mathbb{Q}[x]$, y obtenemos $g = (2x-1)(x^3 - 4x + 2)$. El polinomio $x^3 - 4x + 2$ es primitivo, de grado 3, y no tiene raíces en $\mathbb{Q}$ (las únicas posibles son ± 1 y ± 2, y no lo son), luego es irreducible. Así que la factorización en irreducibles de f en $\mathbb{Z}[x]$ es

$$f = 2 \cdot 5 \cdot (2x-1) \cdot (x^3 - 4x + 2).$$

La factorización en $\mathbb{Q}[x]$ sería la misma, solo que 10 es una unidad. Si tomamos como conjunto representativo de los irreducibles en $\mathbb{Q}[x]$ el conjunto P de los irreducibles monicos, la factorización sería

$$f = 20\Big(x - \frac{1}{2}\Big)(x^3 - 4x + 2).$$

2. *Factorizar $f = x^3 + \frac{1}{2}x^2 - x + 3$ en $\mathbb{Q}[x]$.* Pongamos $f = \frac{1}{2}g$ con $g = 2x^3 + x^2 - 2x + 6 \in \mathbb{Z}[x]$ primitivo. Sus posibles raíces en $\mathbb{Q}$ son ± 1, ± 2, ± 3, ± 6, $\pm\frac{1}{2}$ y $\pm\frac{3}{2}$. Probando, vemos que $g(\frac{3}{2}) = 0$, y por tanto $(2x-3)/g$ en $\mathbb{Z}[x]$. Haciendo la división en $\mathbb{Q}[x]$, obtenemos que $g = (2x-3)(x^2 - 2x + 2)$. El polinomio $x^2 + 2x + 2$ no tiene raíces en $\mathbb{Q}$, y es por tanto irreducible. Así que la factorización buscada es

$$f = \frac{1}{2}(2x-3)(x^2 - 2x + 2) = \Big(x - \frac{2}{3}\Big)(x^2 - 2x + 2).$$

• *El criterio de reducción módulo un primo.* Sea $R_p : \mathbb{Z} \to \mathbb{Z}_p$ el homomorfismo que asigna a cada entero su resto módulo un primo p de $\mathbb{Z}$. Tendremos el homomorfismo inducido $R_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, tal que $R_p(\sum_{i\geq 0} a_i x^i) = \sum_{i\geq 0} R_p(a_i)x^i$.

Proposición 6.4.14. *Sea $f \in \mathbb{Z}[x]$ tal que $R_p(f)$ y f tienen el mismo grado. Si $R_p(f)$ no tiene divisores de grado r, con $0 < r < gr(f)$, en $\mathbb{Z}_p[x]$, entonces f tampoco tiene divisores de grado r en $\mathbb{Z}[x]$. En particular, si f es primitivo y $R_p(f)$ es irreducible, entonces f es irreducible.*

DEMOSTRACIÓN. Supongamos que fuera $f = gh$ en $\mathbb{Z}[x]$, con $gr(g) = r$ y, digamos, $gr(h) = s$, de manera que $r + s = gr(f)$. Tendríamos también que $R_p(f) = R_p(g)\,R_p(h)$. Como, obviamente $gr(R_p(g)) \leq r$ y $gr(R_p(h)) \leq s$, y $gr(R_p(f)) = gr(f) = r + s = gr(R_p(g)) + gr(R_p(h))$, necesariamente $gr(R_p(g)) = r$, lo que es imposible por hipótesis. □

EJEMPLOS. 1. *El polinomio $f = x^4 + 3x^2 - 2x + 5$ es irreducible en $\mathbb{Z}[x]$ (y en $\mathbb{Q}[x]$).*

Su reducido módulo 2, $R_2(f) = x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$ no tiene raíces y por tanto no tiene divisores de grado 1 ni de grado 3. Luego f tampoco los tiene. (Esto también se podría ver directamente viendo que ninguna de las posibles raíces de f en $\mathbb{Q}$, $\pm 1, \pm 5$ lo es). Las únicas posibilidades para f, que es primitivo, es que sea irreducible o factorize como producto de dos irreducibles de grado 2. $R_2(f)$ si tiene, sin embargo, divisores de grado 2, pues $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ es su factorización en irreducibles y no obtenemos información sobre los posibles factores irreducibles de grado dos de f. Pero podemos considerar $R_3(f) = x^4 + x + 2 \in \mathbb{Z}_3[x]$. Este resulta irreducible, pues no tiene raíces y al dividirlo por los tres irreducibles de grado 2 los restos son no nulos. Luego $R_3(f)$ es irreducible y, por tanto, f también lo es. □

2. *El polinomio $f = x^4 + 3x^3 + 5x^2 + 1$ es irreducible en $\mathbb{Z}[x]$ (y en $\mathbb{Q}[x]$).*

Su reducido módulo 2, $R_2(f) = x^4 + x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ tiene a 1 como raíz, y descompone como $R_2(f) = (x+1)(x^3 + x + 1)$. El polinomio $(x^3 + x + 1) \in \mathbb{Z}_2[x]$ es de grado 3 y no tiene raíces, luego es irreducible. Así que la anterior es la factorización de $R_2(f)$ en irreducibles. Claramente entonces $R_2(f)$ no tiene divisores de grado 2, luego f tampoco los tiene en $\mathbb{Z}[x]$. Las únicas posibilidades para f, que es primitivo, es que sea irreducible o factorize como producto de uno de grado uno por uno de grado 3. Pero no tiene raíces en $\mathbb{Q}$, ya que las únicas posibles son ± 1, y no lo son. Luego f es irreducible. □

3. *El polinomio* $\phi = \frac{2}{9}x^6 + \frac{2}{3}x^5 - \frac{2}{9}x^4 + \frac{2}{3}x^3 + \frac{2}{3}x^2 + \frac{2}{3}x - \frac{2}{9}$ *es irreducible en* $\mathbb{Q}[x]$.

Como $\phi = \frac{2}{9}f$, con $f = x^6 + 3x^5 - x^4 + 3x^2 + 3x - 1$, ϕ será irreducible en $\mathbb{Q}[x]$ si y solo si f lo es en $\mathbb{Z}[x]$. Ahora, $R_2(f) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ factoriza como producto de irreducibles en $\mathbb{Z}_2[x]$ como $R_2(f) = (x^3 + x + 1)(x^3 + x^2 + 1)$. Podemos concluir entonces que f no tiene divisores de grado 1, 2, 4 o 5 en $\mathbb{Z}[x]$. $R_3(f) = x^6 - x^4 - 1$ factoriza como producto de irreducibles en $\mathbb{Z}_3[x]$ como $R_3(f) = (x^2 + 1)(x^4 + x^2 - 1)$, lo que nos permite concluir que f no tiene divisores en $\mathbb{Z}[x]$ de grado 3. Luego f es irreducible, ya que no tiene divisores de grado 0 al ser primitivo.

4. *Factorizar* $f = x^5 + 8x^4 + 18^3 + 11x^2 + 7x + 3$ *en* $\mathbb{Z}[x]$. Sus posibles raíces son ± 1 y ± 3. Probando, vemos que $f(-3) = 0$. Dividiendo en $\mathbb{Q}[x]$, obtenemos que $f = (x+3)g$, con $g = x^4 + 5x^3 + 3x^2 + 2x + 1$. Las posibles raíces de g en $\mathbb{Q}$ son ± 1, y comprobamos que ninguna lo es. Luego g no tiene divisores de grado 1 ni de grado 3. Considerando $R_2(g) = x^4 + x^3 + x^2 + 1$, vemos que tiene a 1 como raíz y que factoriza en irreducibles en $\mathbb{Z}_2[x]$ como $R_2(g) = (x+1)(x^3 + x + 1)$, de donde concluimos que $R_2(g)$, y entonces g, no tiene divisores de grado 2. Luego g es irreducible y la factorización buscada es $f = (x+3)(x^4 + x^3 + x^2 + 1)$.

- *El criterio de Eisenstein*.

Proposición 6.4.15. *Sea* $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, *con* $a_n \neq 0$, *un polinomio primitivo. Entonces* f *es irreducible si existe un primo* $p \in \mathbb{Z}$ *verificando cualquiera de las siguientes condiciones:*

1. p/a_i *para todo* $i = 0, 1, \ldots, n-1$, *y* p^2 *no divide a* a_0.
2. p/a_i *para todo* $i = 1, \ldots, n$, *y* p^2 *no divide a* a_n.

DEMOSTRACIÓN. Lo demostramos en el primer supuesto. La demostración para el segundo es paralela. Supongamos $f = gh$ con $g = b_0 + b_1x + \cdots + b_rx^r$ y $h = c_0 + c_1x + \cdots + c_rx^s$, donde $b_r \neq 0 \neq c_s$ y $r, s \geq 1$. Como p/a_0 y $a_0 = b_0c_0$, p tiene que dividir a b_0 o a c_0. Pero como p^2 no divide a a_0, p no puede dividir simultáneamente a ambos. Supongamos que p/b_0, y entonces no a c_0. Como f es primitivo, y p divide a todos los coeficientes en grados menores que n, p no puede dividir a $a_n = b_rc_s$. Por tanto que p no divide ni a b_r ni a c_s. Sea i el primer natural tal que p no divide a b_i. sera $0 < i < n$, pues p/b_0 e $i \leq r < n$. Como el coeficiente a_i de f es

$$a_i = b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c1 + b_ic_0$$

y p/a_i, concluimos que p/b_ic_0. Pero p es primo y p no divide ni a b_i ni a c_0, esto es una contradicción. □

EJEMPLOS. 1. *El polinomio* $2x^5 - 6x^3 + 9x^2 - 15$ *es irreducible en* $\mathbb{Z}[x]$ *(y en* $\mathbb{Q}[x]$*)* (por el criterio de Eisenstein para el primo $p = 3$.)

2. *El polinomio* $3x^7 - 6x^5 + 14x^2 - 10x^2 + 2x - 18$ *es irreducible en* $\mathbb{Z}[x]$ *(y en* $\mathbb{Q}[x]$*)* (por el criterio de Eisenstein para el primo $p = 2$.)

3. *El polinomio* $6x^4 + 9x^3 - 3x^2 + 10$ *es irreducible en* $\mathbb{Z}[x]$ *(y en* $\mathbb{Q}[x]$*)* (por el criterio de Eisenstein para el primo $p = 3$.

4. *El polinomio* $3x^7-70x^3+140$ *es irreducible en* $\mathbb{Z}[x]$ *(y en* $\mathbb{Q}[x]$*)* (por el criterio de Eisenstein para el primo $p=7$. Observar que no vale el primo $p=2$ para aplicar el criterio, pues $140=5\cdot 4\cdot 7$.)

• *Traslación en la indeterminada*. Sea $a\in\mathbb{Z}$ y $T_a:\mathbb{Z}[x]\to\mathbb{Z}[x]$ el homomorfismo es la identidad en los coeficientes y asigna a x el binomio $T_a(x)=x+a$. Esto es,

$$T_a\Big(\sum_{i\geq 0} a_i x^i\Big)=\sum_{i\geq 0} a_i(x+a)^i.$$

Es fácil ver que T_a es un isomorfismo, con inverso T_{-a}. Además, para cualquier $f\in\mathbb{Z}[x]$, f y $T_a(f)$ tienen el mismo grado.

Proposición 6.4.16. *Sea* $f\in\mathbb{Z}[x]$. *Si* $T_a(f)$ *es irreducible para algún* $a\in\mathbb{Z}$, *entonces* f *también lo es.*

Demostración. Si f tuviera un divisor propio, digamos g, entonces sería $f=gh$ para un cierto $h\in\mathbb{Z}[x]$, donde ni g ni h son ± 1. Entonces, tendríamos también que $T_a(f)=T_a(g)T_a(h)$, donde ni $T_a(g)$ ni $T_a(h)$ son ± 1, lo que estaría en contradicción con el supuesto de que $T_a(f)$ es irreducible. ■

EJEMPLO. *El polinomio* $f=x^4+1$ *es irreducible en* $\mathbb{Z}[x]$ *(y en* $\mathbb{Q}[x]$*).*

$T_1(x^4+1)=(x+1)^4+1=x^4+4x^3+6x^2+4x+2$, que es irreducible por Eisenstein para $p=2$.