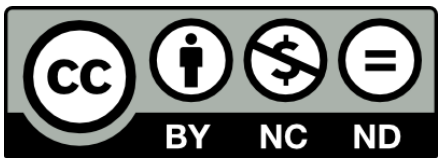
Álgebra I

Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



Álgebra I

Los Del DGIIM, losdeldgiim.github.io

José Juan Urrutia Milán "JJ"
Arturo Olivares Martos

Granada, 2023

Índice general

1. El lenguaje de los conjuntos

En este primer tema, abordaremos un desarrollo sencillo de la teoría de conjuntos, basado en los axiomas de Zermelo-Fraenkel. El autor puede adentrarse en este campo gracias al libro *Naive Set Theory*, de Paul Halmos, cuya lectura recomendamos. En este documento no haremos un desarrollo tan exhaustivo desde la axiomática por falta de tiempo. Es por tanto que daremos al principio algunas definiciones basadas en la intuición del matemático que inicia este curso.

1.1. Conceptos básicos

Definición 1.1 (Conjunto)**.** Llamaremos **conjunto** a una colección de objetos (a los que también llamaremos **elementos**) en la que no influye el orden.

Notación. Usualmente, notaremos a los conjuntos con letras mayúsculas y a los elementos con letras minúsculas, pudiendo haciendo uso incluso de letras griegas.

Si A es un conjunto y a es un elemento suyo, diremos que *a pertenece a A*, notado $a \in A$; mientras que si a no es un elemento de A, diremos que *a no pertenece a A*, notado $a \notin A$.

A la hora de definir un conjunto, es necesario hacerlo por *extensión*, proporcionando todos sus elementos; o por *comprensión*, proporcionando una regla que cumplan todos los elementos que pertenecen al conjunto. Por ejemplo, las siguientes definiciones son equivalentes:

$$X = \{0, 1, 2, 3, 4, 5\}$$
$$X = \{x \mid x \in \mathbb{N} \ \wedge \ x < 6\}$$

Si X es un conjunto finito con elementos $a_1, a_2, \ldots, a_n$, es habitual escribir: $X = \{a_1, a_2, \ldots, a_n\} = \{a_i \mid 1 \leqslant i \leqslant n\} = \{a_i\}_{i=1,\ldots,n}$. Notemos que, en este ejemplo, X tiene n elementos.

Definición 1.2 (Cardinal)**.** Al número n de elementos de un conjunto le llamaremos **cardinal del conjunto**. Si X es un conjunto, notaremos a su cardinal por $|X|$ ó por $\#X$:

$$|X| = \#X = n$$

Diremos que dos conjuntos X e Y son iguales (notado $X = Y$) si tienen los mismos elementos, ya que un conjunto está totalmente definido por sus elementos. Por otra parte, si $\exists\ x \in X$ tal que $x \notin Y$, o bien $\exists\ y \in Y$ tal que $y \notin X$, diremos

que X e Y son distintos: $X \neq Y$.

Además, admitimos la existencia de un conjunto vacío (notado $\emptyset$), como aquel conjunto con cardinal 0 ($|\emptyset| = 0$). Es decir, $\emptyset$ no tiene elementos, luego nunca será posible encontrar un elemento x de forma que[1] $x \in \emptyset$.

Definición 1.3 (Subconjunto)**.** Dados dos conjuntos X e Y, diremos que X **es un subconjunto de** Y si todo elemento de X es también un elemento de Y. Es decir:

$$\forall x \in X \Rightarrow x \in Y$$

Lo notaremos como $X \subseteq Y$. En dicho caso, podremos decir también que X **está contenido en** Y.

Algunas consecuencias inmediatas de fácil comprobación son:

- $X = Y \iff X \subseteq Y \ \wedge \ Y \subseteq X$.
- $\emptyset \subseteq X$ para todo conjunto X.
- $X \subseteq X$ para todo conjunto X.
- La notación $X \subset Y$ es equivalente a la de $X \subseteq Y$.

Definición 1.4 (Subconjunto propio)**.** Si $X \neq \emptyset$ es un conjunto tal que se tiene $X \subseteq Y \ \wedge \ X \neq Y$ diremos que X es un subconjunto propio de Y. Es decir, X es un subconjunto propio de Y si:

1. $\forall x \in X \Rightarrow x \in Y$
2. $\exists y \in Y \mid y \notin X$

En dicho caso, lo notaremos por $X \subsetneq Y$.

Notemos que los únicos subconjuntos no propios de un conjunto X son X y $\emptyset$.

Definición 1.5 (Partes de un conjunto)**.** Dado cualquier conjunto X, podremos formar un nuevo conjunto, que notaremos como $\mathcal{P}(X)$ y llamaremos **conjunto partes de** X ó **conjunto potencia de** X al conjunto cuyos elementos son cada uno de los posibles subconjuntos de X que podamos formar:

$$\mathcal{P}(X) = \{A \mid A \subseteq X\}$$

De la definición, se deduce que $\emptyset, X \in \mathcal{P}(X)$ para todo conjunto X.

Ejemplo. Algunos ejemplos del conjunto de las partes de X son:

1. $X = \{1, 2, 3\}$

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, X\}$$

[1] Esta observación no parece de mucha relevancia, pero gran número de demostraciones se basan en llegar a contradicción viendo que un elemento pertenece al conjunto vacío. Se dice que son demostraciones "por vacuidad".

2. $X = \emptyset$

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$
$$\mathcal{P}[\mathcal{P}(\emptyset)] = \mathcal{P}[\{\emptyset\}] = \{\emptyset, \{\emptyset\}\}$$

Notemos que, dado un conjunto X, el conjunto $\mathcal{P}(X)$ es el primer ejemplo de conjunto que a su vez contiene a conjuntos. El alumno puede llegar a confundirse con qué notación usar en cada caso. El siguiente ejemplo muestra un caso básico de la notación que debemos usar al trabajar con distintos tipos de elementos matemáticos.

Ejemplo. Si X es un conjunto, x es un elemento suyo ($x \in X$) y consideramos el conjunto partes de X, $\mathcal{P}(X)$. Podremos escribir:

$$x \in X \qquad \{x\} \subseteq X \qquad \{x\} \in \mathcal{P}(X) \qquad X \in \mathcal{P}(X)$$

Pero **no** podremos escribir:

$$\{x\} \in X \qquad x \subseteq X \qquad \{x\} \subseteq \mathcal{P}(X) \qquad X \subseteq \mathcal{P}(X)$$

Durante la carrera de matemáticas se verán numerosos ejemplos de conjuntos que a su vez contienen a conjuntos (y dichos conjuntos quizás contendrán otros conjuntos), basta considerar el conjunto $\mathcal{P}(\mathcal{P}(X))$ para cualquier conjunto X.

Será usual denotar por "familia" a los conjuntos cuyos elementos son a su vez conjuntos. Como notación para estos, se suelen usar letras estilográficas ($\mathcal{A}, \mathcal{B}, \ldots$), o en ocasiones por letras griegas mayúsculas, aunque siempre podremos saber la naturaleza del conjunto gracias a cómo esté definido.

Definición 1.6 (Intersección)**.** Sea X un conjunto y sean $A, B \in \mathcal{P}(X)$, definimos la **intersección** de A y de B, notado $A \cap B$ como el subconjunto de X formado por aquellos elementos que pertenecen simultáneamente a A y a B:

$$A \cap B = \{x \in X \mid x \in A \ \wedge \ x \in B\}$$

Definición 1.7 (Unión)**.** Sea X un conjunto y sean $A, B \in \mathcal{P}(X)$, definimos la **unión** de A y de B, notado $A \cup B$ como el subconjunto de X formado por aquellos elementos que pertenecen a A o a B:

$$A \cup B = \{x \in X \mid x \in A \ \vee \ x \in B\}$$

Cuando el conjunto X esté claro por el contexto podremos mencionar simplemente la intersección o unión de dos conjuntos, sin determinar de forma explícita el conjunto X del que ambos son subconjuntos.

Definición 1.8 (Disjuntos)**.** Sea X un conjunto y sean $A, B \in \mathcal{P}(X)$, diremos que A **y** B **son disjuntos** si $A \cap B = \emptyset$.

Proposición 1.1. *Sea X un conjunto y $A, B, C \in \mathcal{P}(X)$. Algunas de las propiedades que se verifican sobre conjuntos son:*

1. *Propiedad conmutativa:*

$$A \cap B = B \cap A \quad ; \quad A \cup B = B \cup A$$

2. *Propiedad asociativa:*

$$A \cap (B \cap C) = (A \cap B) \cap C \quad ; \quad A \cup (B \cup C) = (A \cup B) \cup C$$

3. *Propiedad de la idempotencia:*

$$A \cap A = A \quad ; \quad A \cup A = A$$

4. *Propiedad distributiva:*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad ; \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Demostración. Demostramos cada una de las propiedades por separado:

1. Propiedad conmutativa:

$$A \cap B = \{x \in X \mid x \in A \ \wedge \ x \in B\} = \{x \in X \mid x \in B \ \wedge \ x \in A\} = B \cap A$$
$$A \cup B = \{x \in X \mid x \in A \ \vee \ x \in B\} = \{x \in X \mid x \in B \ \vee \ x \in A\} = B \cup A$$

2. Propiedad asociativa:

$$\begin{aligned} A \cap (B \cap C) &= A \cap \{x \in X \mid x \in B \ \wedge \ x \in C\} = \\ &= \{x \in X \mid x \in A \ \wedge \ x \in B \ \wedge \ x \in C\} = \\ &= \{x \in X \mid x \in A \ \wedge \ x \in B\} \cap C = \\ &= (A \cap B) \cap C \end{aligned}$$

$$\begin{aligned} A \cup (B \cup C) &= A \cup \{x \in X \mid x \in B \ \vee \ x \in C\} = \\ &= \{x \in X \mid x \in A \ \vee \ x \in B \ \vee \ x \in C\} = \\ &= \{x \in X \mid x \in A \ \vee \ x \in B\} \cup C = \\ &= (A \cup B) \cup C \end{aligned}$$

3. Propiedad de la idempotencia:

$$A \cap A = \{x \in X \mid x \in A \ \wedge \ x \in A\} = \{x \in X \mid x \in A\} = A$$
$$A \cup A = \{x \in X \mid x \in A \ \vee \ x \in A\} = \{x \in X \mid x \in A\} = A$$

4. Propiedad distributiva:

$$\begin{aligned} A \cap (B \cup C) &= A \cap \{x \in X \mid x \in B \ \vee \ x \in C\} = \\ &= \{x \in X \mid x \in A \ \wedge \ (x \in B \ \vee \ x \in C)\} = \\ &= \{x \in X \mid (x \in A \ \wedge \ x \in B) \ \vee \ (x \in A \ \wedge \ x \in C)\} = \\ &= \{x \in X \mid x \in A \ \wedge \ x \in B\} \cup \{x \in X \mid x \in A \ \wedge \ x \in B\} = \\ &= (A \cap B) \cup (A \cap C) \end{aligned}$$

$$\begin{aligned} A \cup (B \cap C) &= A \cup \{x \in X \mid x \in B \ \wedge \ x \in C\} = \\ &= \{x \in X \mid x \in A \ \vee \ (x \in B \ \wedge \ x \in C)\} = \\ &= \{x \in X \mid (x \in A \ \vee \ x \in B) \ \wedge \ (x \in A \ \vee \ x \in C)\} = \\ &= \{x \in X \mid x \in A \ \vee \ x \in B\} \cap \{x \in X \mid x \in A \ \vee \ x \in B\} = \\ &= (A \cup B) \cap (A \cup C) \end{aligned}$$

□

Definición 1.9 (Uniones e intersecciones generalizadas)**.** Sea X un conjunto, y consideramos $\Gamma \subseteq \mathcal{P}(X)$ una familia de subconjuntos de X. Definimos la unión y la intersección de todos los elementos de Γ por:

$$\bigcap_{A\in\Gamma} A = \{x \in X \mid x \in A \ \ \forall A \in \Gamma\}$$
$$\bigcup_{A\in\Gamma} A = \{x \in X \mid \exists A \in \Gamma \mid x \in A\}$$

A veces, simplemente lo notaremos por:

$$\bigcap \Gamma = \bigcap_{A\in\Gamma} A$$
$$\bigcup \Gamma = \bigcup_{A\in\Gamma} A$$

Notemos que si Γ es una familia finita: $\Gamma = \{A_1, A_2, \ldots, A_n\} \subseteq \mathcal{P}(X)$, entonces:

$$\bigcap_{A\in\Gamma} A = A_1 \cap A_2 \cap \ldots \cap A_n \qquad \bigcup_{A\in\Gamma} A = A_1 \cup A_2 \cup \ldots \cup A_n$$

En el caso anterior, podemos notar:

$$\bigcap_{A\in\Gamma} A = \bigcap_{i=1}^{n} A_i \qquad \bigcup_{A\in\Gamma} A = \bigcup_{i=1}^{n} A_i$$

Ejemplo. Sea $X = \{0, 1, 2, 3, 4, 5\}$, y consideramos $\Gamma = \{\{0, 1\}, \{1, 2\}, \{1, 3, 5\}\} \subseteq \mathcal{P}(X)$:

$$\bigcap_{A\in\Gamma} A = \{1\} \qquad \bigcup_{A\in\Gamma} A = \{0, 1, 2, 3, 5\}$$

Definición 1.10 (Complementario)**.** Sea X un conjunto y $A \in \mathcal{P}(X)$, definimos el **complementario de A en X**, notado $X - A$ o $X \setminus A$, como el subconjunto de X formado por aquellos elementos de X que no pertenezcan a A:

$$X - A = \{x \in X \mid x \notin A\}$$

Notación. Cuando el conjunto X sea claro por el contexto (por ejemplo, cuando estemos trabajando continuamente con números reales), notaremos simplemente $\overline{A}$ o $C(A)$ (que será equivalente a escribir $X - A$).

Ejemplo. Sea $A = \{x \in \mathbb{N} \mid x \geqslant 4\} \subseteq \mathbb{N}$:

$$\mathbb{N} - A = \{0, 1, 2, 3\} = \{x \in \mathbb{N} \mid x < 4\}$$
$$\mathbb{Z} - A = \{x \in \mathbb{Z} \mid x < 4\}$$

Proposición 1.2. *Sea X un conjunto y $A \in \mathcal{P}(X)$. Algunas propiedades que se verifican sobre el complementario son:*

1. $C(\emptyset) = X$.
2. $C(X) = \emptyset$.
3. $A \cup C(A) = X$.
4. $A \cap C(A) = \emptyset$.
5. $C(C(A)) = A$.

Demostración. Demostramos cada una de las propiedades por separado:

1. $C(\emptyset) = \{x \in X \mid x \notin \emptyset\} = \{x \in X\} = X$.
2. $C(X) = \{x \in X \mid x \notin X\} = \emptyset$.
3. $A \cup C(A) = \{x \in X \mid x \in A \ \vee \ x \notin A\} = \{x \in X\} = X$.
4. $A \cap C(A) = \{x \in X \mid x \in A \ \wedge \ x \notin A\} = \emptyset$.
5. $C(C(A)) = \{x \in X \mid x \notin C(A)\} = \{x \in X \mid x \in A\} = A$.

□

Proposición 1.3 (Leyes de De Morgan)**.** *Sea X un conjunto con $A, B \in \mathcal{P}(X)$, se verifica que:*

1. $C(A \cup B) = C(A) \cap C(B)$
2. $C(A \cap B) = C(A) \cup C(B)$

Demostración. Demostramos cada una de las igualdades:

1. $C(A \cup B) = C(A) \cap C(B)$:

$$\begin{aligned} C(A \cup B) &= \{x \in X \mid x \notin A \cup B\} = \\ &= \{x \in X \mid x \notin \{x \in X \mid x \in A \ \vee \ x \in B\}\} = \\ &= \{x \in X \mid x \notin A \ \wedge \ x \notin B\} = \\ &= \{x \in X \mid x \notin A\} \cap \{x \in X \mid x \notin B\} = C(A) \cap C(B) \end{aligned}$$

2. $C(A \cap B) = C(A) \cup C(B)$:

$$\begin{aligned} C(A \cap B) &= \{x \in X \mid x \notin A \cap B\} = \\ &= \{x \in X \mid x \notin \{x \in X \mid x \in A \ \wedge \ x \in B\}\} = \\ &= \{x \in X \mid x \notin A \ \vee \ x \notin B\} = \\ &= \{x \in X \mid x \notin A\} \cup \{x \in X \mid x \notin B\} = C(A) \cup C(B) \end{aligned}$$

□

Proposición 1.4 (Leyes de De Morgan generalizadas)**.** *Sea X un conjunto, $\Gamma \subseteq \mathcal{P}(X)$, se verifica:*

1. *El complementario de la unión es la intersección de los complementarios.*

$$C\left(\bigcup_{A\in\Gamma} A\right) = \bigcap_{A\in\Gamma} C(A)$$

2. *El complementario de la intersección es la unión de los complementarios.*

$$C\left(\bigcap_{A\in\Gamma} A\right) = \bigcup_{A\in\Gamma} C(A)$$

Demostración. Demostramos cada igualdad por separado:

1. $C\left(\bigcup_{A\in\Gamma} A\right) = \left\{x \in X \mid x \notin \bigcup_{A\in\Gamma} A\right\} = \{x \in X \mid x \notin A \ \forall A \in \Gamma\} = \bigcap_{A\in\Gamma} C(A)$
2. $C\left(\bigcap_{A\in\Gamma} A\right) = \left\{x \in X \mid x \notin \bigcap_{A\in\Gamma} A\right\} = \{x \in X \mid \exists A \in \Gamma \mid x \notin A\} = \bigcup_{A\in\Gamma} C(A)$

□

Definición 1.11 (Complementario generalizado)**.** Sea X un conjunto y consideramos $A, B \in \mathcal{P}(X)$, definimos **el complementario de** A **en** B, notado $B - A$ como el conjunto:

$$B - A = \{x \in X \mid x \in B \ \wedge \ x \notin A\} = B \cap C(A)$$

Proposición 1.5 (Propiedad distributiva generalizada)**.** *Sea X un conjunto con $B \in \mathcal{P}(X)$ y $\Gamma \subseteq \mathcal{P}(X)$, se tiene que:*

$$B \cap \left(\bigcup_{A\in\Gamma} A\right) = \bigcup_{A\in\Gamma} (B \cap A) \qquad B \cup \left(\bigcap_{A\in\Gamma} A\right) = \bigcap_{A\in\Gamma} (B \cup A)$$

Demostración.

$$\begin{aligned} B \cap \left(\bigcup_{A\in\Gamma} A\right) &= \left\{x \in X \mid x \in B \ \wedge \ x \in \bigcup_{A\in\Gamma} A\right\} = \\ &= \{x \in X \mid x \in B \ \wedge \ \exists A \in \Gamma \mid x \in A\} = \\ &= \{x \in X \mid \exists A \in \Gamma \mid x \in B \ \wedge \ x \in A\} = \bigcup_{A\in\Gamma} (B \cap A) \end{aligned}$$

$$\begin{aligned} B \cup \left(\bigcap_{A\in\Gamma} A\right) &= \left\{x \in X \mid x \in B \ \vee \ x \in \bigcap_{A\in\Gamma} A\right\} = \\ &= \{x \in X \mid x \in B \ \vee \ x \in A \ \forall A \in \Gamma\} = \\ &= \{x \in X \mid \forall A \in \Gamma \ x \in B \ \vee \ x \in A\} = \bigcap_{A\in\Gamma} (B \cup A) \end{aligned}$$

□

1.2. Álgebra de proposiciones

Definición 1.12 (Conjunto que verifica una propiedad)**.** Sea X un conjunto y sea P una propiedad referida a los elementos de dicho conjunto, definimos el conjunto de elementos de X que verifica dicha propiedad, que usualmente notaremos por X_P, como:

$$X_P = \{x \in X \mid x \text{ verifica } P\}$$

Ejemplo. Sea $X = \mathbb{Z}$, y sea P la propiedad de ser un número positivo. Entonces:

$$X_P = \{x \in \mathbb{Z} \mid x \geqslant 0\} = \mathbb{N}$$

Proposición 1.6. *Sea X un conjunto y sean P y Q dos propiedades referidas a dicho conjunto. Nos es posible calcular el conjunto de elementos de X que verifican P y Q simultáneamente o el conjunto de elementos de X que verifica sólo una propiedad a partir de la fórmula:*

$$X_{(P \wedge Q)} = X_P \cap X_Q$$
$$X_{(P \vee Q)} = X_P \cup X_Q$$

Demostración. Trivialmente, se verifica lo siguiente:

$$X_P \cap X_Q = \{x \in X \mid x \text{ verifica } P \ \wedge \ x \text{ verifica } Q\} = X_{(P \wedge Q)}$$
$$X_P \cup X_Q = \{x \in X \mid x \text{ verifica } P \ \vee \ x \text{ verifica } Q\} = X_{(P \vee Q)}$$

□

Proposición 1.7. *Sea X un conjunto y sea P una propiedad referida a dicho conjunto, podemos calcular el conjunto de elementos de X que no cumplen la propiedad P a partir de X_P, de la forma:*

$$X_{\neg P} = C(X_P)$$

Demostración.

$$C(X_P) = \{x \in X \mid x \notin X_P\} = \{x \in X \mid x \text{ no verifica } P\} = X_{\neg P}$$

□

Definición 1.13 (Proposición matemática)**.** Una **proposición matemática** es una relación entre dos propiedades P y Q referidas a los elementos de un conjunto X del tipo

$$P \Longrightarrow Q$$

Se lee "P implica Q" o "P entonces Q", y significa que si $x \in X$ verifica P, entonces también verifica Q. Equivalentemente, ha de ser $X_P \subseteq X_Q$.

Definición 1.14 (Recíproco)**.** Dada una proposición matemática $P \Longrightarrow Q$, definimos su **proposición matemática recíproca**, o **recíproco** como la proposición matemática:

$$Q \Longrightarrow P$$

Observación. Dada una proposición matemática, su recíproco no siempre es verdadero. Por ejemplo, es cierto que todo número natural es un número entero ($\mathbb{N} \subseteq \mathbb{Z}$) pero su recíproco, que todo número entero es un número natural, no es cierto ($\mathbb{Z} \nsubseteq \mathbb{N}$).

Definición 1.15 (Contrarrecíproco)**.** Dada una proposición matemática $P \Longrightarrow Q$, definimos su **proposición matemática contrarrecíproca**, o **contrarrecíproco** como la proposición matemática:

$$\neg Q \Longrightarrow \neg P$$

Proposición 1.8 (Transitividad)**.** *Sean P, Q, R propiedades referidas a los elementos de un conjunto X, tales que $P \Longrightarrow Q$ y $Q \Longrightarrow R$. Entonces:*

$$P \Longrightarrow R$$

Demostración. Se demuestra gracias a la transitividad de los subconjuntos, ya que $X_P \subseteq X_Q \subseteq X_R$, por lo que $X_P \subseteq X_R$. □

Definición 1.16 (Equivalencia)**.** Sea X un conjunto y P y Q propiedades referidas a sus elementos, diremos que P **y** Q **son equivalentes**, notado $P \Longleftrightarrow Q$ y leído "P si y solo si Q", si:

$$P \Longrightarrow Q \quad \wedge \quad Q \Longrightarrow P$$

Notemos que la equivalencia se da cuando tanto una proposición matemática como su proposición recíproca son ciertas.

Proposición 1.9 (Equivalencia generalizada)**.** *Sea X un conjunto y P_1, P_2, ..., P_n propiedades referidas a elementos de X tales que $P_i \Longrightarrow P_{i+1}$ $\forall i \in \{1, \ldots, n-1\}$ y que $P_n \Longrightarrow P_1$. Entonces:*

$$P_i \Longleftrightarrow P_j \quad \forall i, j \in \{1, \ldots, n\}$$

Demostración. $\forall i, j \in \{1, \ldots, n\}$:

- Si $i = j$:
  Se tiene $P_i \Leftrightarrow P_j$ trivialmente, ya que:
  $$X_{P_i} = X_{P_j} \Rightarrow \begin{cases} X_{P_i} \subseteq X_{P_j} & \Longrightarrow & P_i \Rightarrow P_j \\ \wedge & & \wedge \\ X_{P_j} \subseteq X_{P_i} & \Longrightarrow & P_j \Rightarrow P_i \end{cases}$$
  Por tanto, $P_i \Leftrightarrow P_j$.
- Si $i < j$: $(P_i \Rightarrow P_{i+1} \Rightarrow \ldots \Rightarrow P_j) \Rightarrow (P_i \Rightarrow P_j)$
- Si $i > j$: $(P_i \Rightarrow P_n \Rightarrow P_1 \Rightarrow \ldots \Rightarrow P_j) \Rightarrow (P_i \Rightarrow P_j)$

Para la implicación $P_j \Rightarrow P_i$ hágase un camino similar al especificado y se obtendrá $P_j \Leftrightarrow P_i$. □

De esta forma, siempre que queramos probar que un conjunto finito de propiedades matemáticas son equivalentes entre sí, bastará probar que la primera es equivalente a la segunda, la segunda a la tercera, y así hasta que la penúltima es equivalente a la última y finalmente que la última es equivalente a la primera.

Demostración por reducción al absurdo

Sea X un conjunto, P y Q propiedades referidas a los elementos de dicho conjunto. Queremos demostrar que $P \Rightarrow Q$. El procedimiento es el siguiente:

- Supongamos que $\exists x \in X \mid x \in X_P \cap C(X_Q)$, es decir, que $\exists x \in X$ que verifica P pero no Q.
- Si llegamos a una resultado que es falso o que contradice nuestra hipótesis ($x \in C(X_P)$), podemos concluir que $\forall x \in X_P \Longrightarrow x \in X_Q$. Es decir, queda demostrado que $P \Longrightarrow Q$.

Demostración por contrarrecíproco

Lema 1.10. *Sea X un conjunto y $A, B \in \mathcal{P}(X)$. Entonces:*

$$A \subseteq B \Longleftrightarrow C(B) \subseteq C(A)$$

Demostración. Procedemos mediante doble implicación:

$\Longrightarrow$) Supongamos que $x \in C(B) \ \wedge \ x \notin C(A)$, luego $x \notin B \ \wedge \ x \in A$. Como $A \subseteq B$, tenemos que $x \in B$, por lo que llegamos a una contradicción. Por tanto, se tiene que $x \in C(A)$ y, por tanto, $C(B) \subseteq C(A)$.

$\Longleftarrow$) $A = C(C(A)) \subseteq C(C(B)) = B$.

□

Proposición 1.11 (Demostración por contrarrecíproco)**.** *Sea X un conjunto, P y Q propiedades referidas a sus elementos, son equivalentes:*

1. *$P \Rightarrow Q$ (Demostración directa).*
2. *$\neg Q \Rightarrow \neg P$ (Demostración por contrarrecíproco).*

Es decir, dada una proposición matemática, será verdadera si y solo si lo es su proposición matemática contrarrecíproca.

Demostración.

$$(P \Rightarrow Q) \Leftrightarrow X_P \subseteq X_Q \overset{(*)}{\Longleftrightarrow} C(X_Q) \subseteq C(X_P) \Longleftrightarrow (\neg Q \Rightarrow \neg P)$$

donde en $(*)$ he aplicado el lema anterior, el Lema 1.10. □

1.3. Aplicaciones

Definición 1.17 (Par ordenado)**.** Un par ordenado es un conjunto que contiene a dos elementos a y b, notado (a, b) en el que importa el orden. Es decir, si (a, b) y (c, d) son dos pares ordenados:

$$(a, b) = (c, d) \Longleftrightarrow a = c \ \wedge \ b = d$$

Definición 1.18 (Terna)**.** Una terna es un conjunto de tres elementos a, b, c en el que importa el orden, notado por:

$$(a, b, c)$$

Definición 1.19 (n-Upla)**.** Dado un número natural n, podemos generalizar el concepto de par ordenado o de terna a una n-upla, que es un conjunto de n elementos a_1, a_2, ..., a_n en el que importa el orden. A este lo notaremos por:

$$(a_1, a_2, \ldots, a_n)$$

Definición 1.20 (Producto Cartesiano)**.** Sean X e Y dos conjuntos, definimos el **producto cartesiano de X e Y** como el conjunto:

$$X \times Y = \{(x, y) \mid x \in X \ \wedge \ y \in Y\}$$

Por lo general, se tiene que $X \times Y \neq Y \times X$ salvo que $X = Y$.

Definición 1.21 (Producto Cartesiano generalizado)**.** Sean X_1, X_2, ..., X_n conjuntos, definimos el **producto cartesiano de X_1, X_2, ..., X_n** como el conjunto:

$$X_1 \times X_2 \times \ldots \times X_n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in X_i \ \ \forall i = 1, \ldots, n\}$$

Notación. A veces notaremos: $\prod_{i=1}^{n} X_i =: X_1 \times X_2 \times \ldots \times X_n$.

En el caso en el que $X_1 = X_2 = \ldots = X_n$, notaremos $\prod_{i=1}^{n} X_i =: X^n$.

Ejemplo. Sea $X = \{a, b\}$ e $Y = \{1, 2, 3\}$. Entonces:

$$X \times Y = \{(a,1), (a,2), (a,3), (b,1), (b,2), (b,3)\}$$
$$Y \times X = \{(1,a), (1,b), (2,a), (2,b), (3,a), (3,b)\}$$

Proposición 1.12. *Si X e Y son dos conjuntos finitos, entonces $X \times Y$ es finito, con:*

$$|X \times Y| = |X| \ |Y|$$

Demostración. Para cada elemento de X, tenemos que hay $|Y|$ opciones disponibles para completar el par ordenado. Como hay $|X|$ elementos en X, tenemos que en total hay $|X| \ |Y|$ pares ordenados. □

Definición 1.22 (Aplicación)**.** Una **aplicación** es una terna (X, Y, f) donde X es un conjunto llamado **dominio de la aplicación**, Y es otro conjunto **llamado recorrido, rango o codominio de la aplicación** y $f \subseteq X \times Y$ es un conjunto llamado **grafo de la aplicación**. Esta terna ha de cumplir las siguientes propiedades:

1. $\forall x \in X \ \exists y \in Y \mid (x, y) \in f$.
2. $\forall (x, y), (x', y') \in f$, si $x = x' \Rightarrow y = y'$.

Las dos propiedades anteriores son equivalentes a que:

$$\forall x \in X \ \exists_1 y \in Y \mid (x, y) \in f$$

Al único elemento $y \in Y$ que corresponde a un elemento $x \in X$ le llamaremos imagen por f de x (o simplemente f de x), notado $y =: f(x)$. A veces, a dicho elemento $x \mid f(x) = y$ lo llamaremos antiimagen de y.

Cuando tengamos una aplicación (es decir una terna (X, Y, f)), hablaremos de una aplicación f de X en Y, notado de algunas de las siguientes formas:

$$f : X \longrightarrow Y \qquad X \xrightarrow{f} Y$$

Dar una aplicación es dar su dominio, su recorrido y el conjunto de pares ordenados; que es equivalente a dar el dominio, el recorrido y especificar a qué elemento del recorrido le corresponde cada elemento del dominio, que suele ser usual hacerlo mediante una fórmula. Por tanto, dos aplicaciones son iguales si tienen el mismo dominio, recorrido y grafo.

Ejemplo. Algunos ejemplos de la definición anterior son:

1. No existe la aplicación $f : \mathbb{N} \to \mathbb{N}$ dada por $f(x) = x - 1$, ya que no cumple con la primera condición: $f(0) = -1 \notin \mathbb{N}$.

2. No existe la aplicación $g : \mathbb{N} \longrightarrow \mathbb{N}$ definida por la fórmula

$$g(x) = \begin{cases} x & \text{si} \quad x \text{ no es múltiplo ni de 2 ni de 3} \\ \dfrac{x}{2} & \text{si} \quad x \text{ es múltiplo de 2} \\ \dfrac{x}{3} & \text{si} \quad x \text{ es múltiplo de 3} \end{cases}$$

   Esto se debe a que 6 podría tener dos imágenes, por lo que no cumpliría la segunda condición:

$$g(6) = \frac{6}{2} = 3 \qquad g(6) = \frac{6}{3} = 2$$

3. La fórmula $f(x) = \dfrac{x^2 + 1}{x - 1}$ define una aplicación $f :]0, 1[\to \mathbb{R}$ pero no puede definir una aplicación $f : [0, 1] \to \mathbb{R}$, ya que $\nexists f(1)$.

4. La suma de naturales $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ dada por $+(x, y) = x + y$ es una aplicación.

Definición 1.23 (Imagen de una aplicación)**.** Si $f : X \to Y$ es una aplicación, al conjunto de las imágenes de los elementos de X lo llamaremos **conjunto imagen de la aplicación**, notado $Img(f)$:

$$Img(f) = \{f(x) \mid x \in X\} \subseteq Y$$

Definición 1.24 (Sobreyectividad)**.** Dada una aplicación $f : X \to Y$, diremos que f **es sobreyectiva** si $Img(f) = Y$. Es decir, se ha de cumplir que:

$$\forall y \in Y \ \exists x \in X \mid f(x) = y$$

Definición 1.25 (Inyectividad)**.** Dada una aplicación $f : X \to Y$, diremos que f **es inyectiva** si elementos distintos tienen imágenes distintas. Es decir, se ha de cumplir:

$$\forall x, z \in X \mid x \neq z \Rightarrow f(x) \neq f(z)$$

Por contrarrecíproco[2], f es inyectiva si $\forall x, z \in X \mid f(x) = f(z) \Rightarrow x = z$.

Definición 1.26 (Biyectividad)**.** Dada una aplicación $f : X \to Y$, diremos que f **es biyectiva** si es a la vez inyectiva y sobreyectiva.

Definición 1.27 (Conjuntos biyectivos)**.** Sean X e Y dos conjuntos, diremos que son biyectivos, notado $X \cong Y$ ó $X \overset{f}{\cong} Y$ si existe una aplicación $f : X \to Y$ biyectiva.

Ejemplo. Algunos ejemplos de inyectividad, sobreyectividad y biyectividad son:

1. $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^2$ no es sobreyectiva ni inyectiva.
2. $g : \mathbb{Z} \to \mathbb{Z}$, $g(x) = 2x$ es inyectiva pero no sobreyectiva.
3. $h : \mathbb{Z} \to \mathbb{N}$, $h(x) = |x|$ es sobreyectiva pero no inyectiva.
4. $t : \mathbb{Z} \to \mathbb{Z}$, $t(x) = x + 2$ es biyectiva.

Definición 1.28 (Aplicación identidad)**.** Sea X un conjunto, definimos la aplicación **identidad en** X; notada como id_X, I_X, Id_X, o 1_X; como la siguiente aplicación:

$$\begin{array}{rccl} id_X : X & \longrightarrow & X \\ x & \longmapsto & id_X(x) = x \end{array}$$

Definición 1.29 (Composición)**.** Sean $f : X \to Y$ y $g : Y \to Z$ dos aplicaciones, definimos la aplicación g **compuesta con** f, notada $g \circ f$, como la siguiente aplicación:

$$\begin{array}{rccl} g \circ f : X & \longrightarrow & Z \\ x & \longmapsto & g(f(x)) \end{array}$$

Algunas propiedades de la composición de aplicaciones son:

Proposición 1.13. *La composición es asociativa. Es decir, dadas las aplicaciones* $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T$*, se cumple:*

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

Demostración. Los dominios de ambas aplicaciones son X y los codominios T. Falta comprobar que los grafos coinciden. $\forall x \in X$, se cumple que:

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

Por tanto, se tiene $f \circ (g \circ h) = (f \circ g) \circ h$. □

[2]Suele ser la forma más fácil de probar que una aplicación es inyectiva, mediante el contrarrecíproco de la definición.

Proposición 1.14. *Dada una aplicación $f : X \to Y$ arbitraria, se verifica que la identidad es el elemento neutro de la composición. Es decir,*

$$f \circ id_X = f$$
$$id_Y \circ f = f$$

Demostración. Los dominios y codominios de $f \circ id_X$, f, $id_Y \circ f$ coinciden. Falta ver que los grafos también lo hacen. $\forall x \in X$:

$$(f \circ id_X)(x) = f(id_X(x)) = f(x)$$
$$(id_Y \circ f)(x) = id_Y(f(x)) = f(x)$$

Por tanto, $f \circ id_X = f = id_Y \circ f$. □

Lema 1.15. *Sean $f : X \to Y$ y $g : Y \to X$ aplicaciones tales que $g \circ f = id_X$. Entonces, f es inyectiva y g es sobreyectiva.*

Demostración. Demostramos en primer lugar que f es inyectiva:

$$\forall x_1, x_2 \in X \mid f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) = x_1 = x_2$$

Por tanto, como $f(x_1) = f(x_2) \implies x_1 = x_2$, se tiene que f es inyectiva. Veamos ahora que g es sobreyectiva:

$$\forall x \in X \ \exists f(x) \in Y \mid g(f(x)) = x$$

Por tanto, como todo elemento del codominio tiene su antiimagen correspondiente, tenemos que g es inyectiva. □

Teorema 1.16 (Caracterización de la biyectividad)**.** *Sea $f : X \to Y$ una aplicación. Entonces:*

$$f \text{ es biyectiva} \iff \exists g : Y \to X \mid g \circ f = id_X \ \wedge \ f \circ g = id_Y$$

Demostración. $\implies$) Suponemos f biyectiva. Por tanto, $\forall y \in Y \ \exists_1 x \in X \mid f(x) = y$. Definimos $g : Y \to X$ por $g(y) = x \mid f(x) = y$, algo posible ya que, por ser f biyectiva, dicho valor de $x \in X$ es único. Veamos que verifica que $f \circ g = id_Y$:

$$\forall y \in Y \ \ (f \circ g)(y) = f(g(y)) = f(x) = y \Rightarrow f \circ g = id_Y$$

La otra igualdad, de la definición de g se deduce directo, ya que $f(x) = y$:

$$\forall x \in X \ \ (g \circ f)(x) = g(f(x)) = g(y) = x \Rightarrow g \circ f = id_X$$

Por tanto, se tiene esta implicación.

$\impliedby$) Supongamos que $\exists g : Y \to X \mid g \circ f = id_X \ \wedge \ f \circ g = id_Y$. Según el lema anterior, sabemos que:

$$g \circ f = id_X \ \Rightarrow \ f \text{ es inyectiva y } g \text{ es sobreyectiva}$$
$$f \circ g = id_Y \ \Rightarrow \ g \text{ es inyectiva y } f \text{ es sobreyectiva}$$

Por tanto, tenemos que f es biyectiva.

□

Lema 1.17 (Unicidad)**.** *Sea $f : X \to Y$. Si f es biyectiva, se verifica que $g : Y \to X$ es la única aplicación que verifica que $g \circ f = id_X \ \wedge \ f \circ g = id_Y$.*

Demostración. Supongamos que no es única, y sea $h : Y \to X \mid h \circ f = id_X \wedge f \circ h = id_Y$ la otra opción. Entonces:

$$h = h \circ id_Y = h \circ (f \circ g) = (h \circ f) \circ g = id_X \circ g = g$$

Quedando así demostrada la unicidad de g. □

Definición 1.30 (Inversa)**.** Sea $f : X \to Y$ una aplicación biyectiva. Por el lema anterior, sólo existe una aplicación $g : Y \to X \mid g \circ f = id_X \ \wedge \ f \circ g = id_Y$. Llamaremos a esta aplicación g **aplicación inversa de** f y la notaremos como f^{-1}.

Notemos que, dada $f : X \to Y$, para comprobar que $g : Y \to X$ sea la inversa de f, gracias al Lema 1.17 nos basta con ver que $f \circ g = id_Y \ \wedge \ g \circ f = id_X$.

Lema 1.18. *Sea $f : X \to Y$ biyectiva. Entonces f^{-1} es biyectiva, siendo su inversa f:*

$$(f^{-1})^{-1} = f$$

Demostración. f^{-1} es la inversa de f. Por lo que, de manera trivial:

$$f \circ f^{-1} = id_Y$$
$$f^{-1} \circ f = id_X$$

Por lo que dada $f^{-1} \ \exists f \mid f \circ f^{-1} = id_Y \ \wedge \ f^{-1} \circ f = id_X \Rightarrow f^{-1}$ es biyectiva por el Teorema 1.16, siendo $(f^{-1})^{-1} = f$. □

Lema 1.19 (Inversa de una composición)**.** *Sean $f : X \to Y$, $g : Y \to Z$ funciones biyectivas. Entonces:*

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

Demostración. Tenemos que el dominio de ambas es Z y el codominio es X. Aplicamos el Lema 1.17 y la Proposición 1.13:

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = (g \circ id_Y) \circ g^{-1} = g \circ g^{-1} = id_Z$$
$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = (f^{-1} \circ id_Y) \circ f = f^{-1} \circ f = id_X$$

Por lo que:

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

□

Proposición 1.20. *Sea X un conjunto finito no vacío y $f : X \to X$ una aplicación, los siguientes enunciados son equivalentes:*

I. *f es biyectiva.*

II. *f es inyectiva.*

III. *f es sobreyectiva.*

Demostración. Demostramos la siguiente equivalencia:

I $\Longrightarrow$ **II** Trivial, a partir de la definición de aplicación biyectiva.

II $\Longrightarrow$ **III** Sea $f : X \to X$ inyectiva, supongamos que $|X| = n$, $(n \geqslant 1)$. Como f es inyectiva, entonces $|Img(f)| = n$. Luego:

$$Img(f) \subseteq X \ \wedge \ |Img(f)| = |X| \Rightarrow Img(f) = X$$

Por tanto, tenemos que f es sobreyectiva.

III $\Longrightarrow$ **II** Sea f sobreyectiva, y demostraremos que f es inyectiva. Para ello, por reducción al absurdo, supongamos que f no es inyectiva. Por tanto, $|Img(f)| < |X|$. Entonces, $Img(f) \subsetneq X$, llegando así a una contradicción, ya que f era sobreyectiva.

Luego f es inyectiva y como era sobreyectiva, tenemos que es biyectiva.

□

Definición 1.31 (Conjunto imagen de un conjunto)**.** Dada una aplicación $f : X \to Y$ y un conjunto $A \subseteq X$, definimos la imagen de A mediante f, notado por $f_*(A)$ o $f(A)$ por:

$$f(A) = f_*(A) = \{f(x) \mid x \in A\} \subseteq Y$$

Definición 1.32 (Conjunto imagen inversa de un conjunto)**.** Dada una aplicación $f : X \to Y$ y un conjunto $B \subseteq Y$, definimos la imagen inversa de B mediante f, notado por $f^*(B)$ o $f^{-1}(B)$ por:

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

No debemos confundir la notación $f^{-1}(B)$ con la aplicación inversa de f, pues no es necesario suponer nada sobre f para hablar de la imagen inversa del conjunto B.

Proposición 1.21. *La imagen inversa es compatible con todas las operaciones con conjuntos. Sea $f : X \to Y$ una aplicación y $A, B \subseteq Y$, se verifica:*

1. $f^*(A \cup B) = f^*(A) \cup f^*(B)$
2. $f^*(A \cap B) = f^*(A) \cap f^*(B)$
3. $f^*(A - B) = f^*(A) - f^*(B)$
4. $f^*(Y - A) = X - f^*(A)$

Definición 1.33 (Aplicación característica de un conjunto)**.** Sea X un conjunto y $A \subseteq X$, podemos definir la **aplicación característica de** A, notada por χ_A como la aplicación $\chi_A : X \to \{0, 1\}$ dada por:

$$\chi_A(x) = \begin{cases} 1 & \text{si} \quad x \in A \\ 0 & \text{si} \quad x \notin A \end{cases}$$

1.4. Relaciones de equivalencia

Definición 1.34 (Relación binaria)**.** Sea X un conjunto no vacío, una **relación binaria en** X es un subconjunto $R \subseteq X \times X$.

Dados $a, b \in X \mid (a, b) \in R$, diremos que a está relacionado con b por R, notado aRb.

Dada X una relación binaria, algunas propiedades que puede cumplir R son:

- **Reflexividad:** $\forall a \in X \Rightarrow aRa$
- **Simetría:** si: $\forall a, b \in X \mid aRb \Rightarrow bRa$
- **Transitividad:** $\forall a, b, c \in X \mid aRb \ \wedge \ bRc \Rightarrow aRc$

En el caso de que una relación R cumpla las tres propiedades mencionadas, diremos que R **es una relación binaria de equivalencia sobre el conjunto** X.

Ejemplo. Algunos ejemplos de relaciones binarias son:

1. Sea $X = \{a, b, c\}$. Son relaciones binarias:

	Reflexividad	Simetría	Transitividad
$R_1 = \{(a,a), (a,b), (b,c)\}$	No	No	No
$R_2 = \{(a,a), (b,b), (c,c), (a,b), (b,c)\}$	Sí	No	No
$R_3 = \{(a,b), (b,a)\}$	No	Sí	No
$R_4 = \{(a,a), (b,b), (c,c), (a,b), (b,a)\}$	Sí	Sí	Sí

2. Sea $X = \mathbb{N}$, y consideramos la relación binaria:

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a + b \text{ es un número par}\}$$

Veamos que es una relación de equivalencia:

- **Reflexividad:** Sea $a \in X$. Entonces, $aRa \iff a + a = 2a$ es par, lo cual es cierto.
- **Simetría:** Sean $a, b \in X \mid aRb \Longrightarrow a + b = 2k \Longrightarrow b + a = 2k \Longrightarrow bRa$, para cierto $k \in \mathbb{N}$.
- **Transitividad:** $\forall a, b, c \in X \mid aRb \ \wedge \ bRc$, se tiene que $\exists k, k' \in \mathbb{N}$:

$$\left.\begin{array}{ccc} aRb & \Longrightarrow & a + b = 2k \\ \wedge & & \wedge \\ bRc & \Longrightarrow & b + c = 2k' \end{array}\right\} \Longrightarrow a+b+b+c = a+2b+c = 2k+2k' = 2(k+k')$$

Por tanto, se tiene que $a + c = 2(k + k' - b)$, para ciertos $k, k' \in \mathbb{N}$. Por tanto, tenemos que aRc.

3. Sea $X = \mathbb{R}^2$ y definimos $O = (0, 0)$ como el origen del plano cartesiano. Entonces, consideramos la relación binaria:

$$pRq \iff d(O, p) = d(O, q)$$

Aunque la demostración rigurosa de que es una relación de equivalencia no se especifica por superar los conceptos de esta asignatura, es fácil intuir que dos puntos están relacionados si están a la misma distancia del origen; es decir, si pertenecen a la misma circunferencia centrada en el origen.

Definición 1.35 (Clase de equivalencia)**.** Sea X un conjunto no vacío y R una relación binaria de equivalencia. Para cada $a \in X$, definimos **la clase de equivalencia de** a, notada por $\overline{a}$ ó por $[a]$ como el conjunto:

$$[a] = \{x \in X \mid xRa\} \subseteq X$$

Esto es, $[a]$ contiene aquellos elementos de X que estén relacionados o que son equivalentes con a. Por la propiedad reflexiva, tenemos que $aRa \Rightarrow a \in [a]$, por lo que $[a] \neq \emptyset \ \forall a \in X$.

A cada uno de los elementos de X que pertenezcan a $[a]$ para algún $a \in X$ se les llama **representantes de la clase de** a.

Ejemplo. Veamos algunos ejemplos de clase de equivalencia respecto de las relaciones binarias anteriores:

2. Veamos la clase de equivalencia con representante de clase 0 de la relación de equivalencia de los pares:

$$[0] = \{x \in \mathbb{N} \mid xR0\} = \{x \in \mathbb{N} \mid x + 0 \text{ es par}\} = \{x \in \mathbb{N} \mid x \text{ es par}\}$$

3. Veamos la clase de equivalencia con representante de clase el punto $(2, 3)$ de la relación de equivalencia de la distancia:

$$[(2,3)] = \{p \in \mathbb{R}^2 \mid pR(2,3)\} = \{p \in \mathbb{R}^2 \mid d(0,p) = d(0,(2,3))\} = \\ = \left\{p \in \mathbb{R}^2 \mid d(0,p) = \sqrt{13}\right\}$$

Proposición 1.22. *Sea X un conjunto no vacío y R una relación de equivalencia en X. Sean $a, b \in X$. Son equivalentes:*

I. aRb

II. $a \in [b]$

III. $b \in [a]$

IV. $[a] \cap [b] \neq \emptyset$

V. $[a] = [b]$

Demostración. Demostramos por implicaciones sucesivas:

I $\Longrightarrow$ II) Por la definición de $[b]$, tenemos que si $aRb \Rightarrow a \in [b]$.

II $\Longrightarrow$ III) Suponemos $a \in [b]$, es decir, aRb. Por ser una relación de equivalencia, es simétrica, luego bRa, por lo que $b \in [a]$.

III $\Longrightarrow$ IV) Hemos supuesto que $b \in [a]$. Además, se ha visto que $\forall b \in X$, se tiene que $b \in [b]$. Por tanto, $b \in [a] \cap [b]$, por lo que este último no es vacío.

IV $\Longrightarrow$ V) Como $[a] \cap [b] \neq \emptyset \Rightarrow \exists c \in X \mid c \in [a] \cap [b] \Rightarrow cRa \ \wedge \ cRb$.

$$\forall x \in [a] \Rightarrow xRa \overset{cRa}{\Rightarrow} aRc \Rightarrow xRc \overset{cRb}{\Rightarrow} xRb \Rightarrow x \in [b] \Rightarrow [a] \subseteq [b]$$
$$\forall x \in [b] \Rightarrow xRb \overset{cRb}{\Rightarrow} bRc \Rightarrow xRc \overset{cRa}{\Rightarrow} xRa \Rightarrow x \in [a] \Rightarrow [b] \subseteq [a]$$

Tenemos que $[a] \subseteq [b] \ \wedge \ [b] \subseteq [a] \Rightarrow [a] = [b]$.

V $\Longrightarrow$ I) Como $a \in [a] = [b] \Rightarrow aRb$. □

Definición 1.36 (Conjunto cociente)**.** Dado un conjunto X no vacío y una relación de equivalencia R sobre X, se define el **conjunto cociente de X por la relación de equivalencia** R, notado X/R como el conjunto:

$$X/R = \{[a] \mid a \in X\}$$

Ejemplo. Veamos algunos ejemplos de conjuntos cocientes por las relaciones binarias anteriores:

2. Veamos las distintas clases de equivalencia que hay en la relación de equivalencia de los pares:

$$[0] = \{x \in \mathbb{N} \mid xR0\} = \{x \in \mathbb{N} \mid x + 0 \text{ es par}\} = \{x \in \mathbb{N} \mid x \text{ es par}\}$$
$$= \{0, 2, 4, \dots\} \Longrightarrow [0] = [2] = [4] = \dots$$

$$[1] = \{x \in \mathbb{N} \mid xR1\} = \{x \in \mathbb{N} \mid x + 1 \text{ es par}\} = \{x \in \mathbb{N} \mid x \text{ es impar}\}$$
$$= \{1, 3, 5, \dots\} \Longrightarrow [1] = [3] = [5] = \dots$$

Por tanto, $\mathbb{N}/R = \{[0], [1]\}$.

3. Veamos las distintas clases de equivalencia de la relación de equivalencia de la distancia:

$$[p] = \{x \in \mathbb{R}^2 \mid xRp\} = \{x \in \mathbb{R}^2 \mid d(0, x) = d(0, p)\} = \{x \in \mathbb{R}^2 \mid d(0, x) = r\} =$$
$$= C_r \quad \text{(circunferencia de radio } r \text{ y centro } O\text{)}.$$

Por tanto, se tiene que $\mathbb{R}^2/R = \{C_r \mid r \geqslant 0\}$.

Proposición 1.23. *Sea $f : X \to Y$ una aplicación y R una relación de equivalencia en X. Supongamos que f verifica la siguiente propiedad:*

Dados $a, b \in X \mid aRb \Rightarrow f(a) = f(b)$.

Entonces, podemos definir la siguiente aplicación:

$$\begin{array}{rccc} \overline{f} : X/R & \longrightarrow & Y \\ [a] & \longmapsto & \overline{f}([a]) = f(a) \end{array}$$

Se verifica que:

1. *$Img(\overline{f}) = Img(f)$.*
2. *$\overline{f}$ es sobreyectiva $\iff$ f es es sobreyectiva.*
3. *$\overline{f}$ es inyectiva $\iff$ $\forall a, b \in X \mid f(a) = f(b) \Rightarrow aRb$.*

Demostración. Veamos en primer lugar que $\overline{f}$ está bien definida, es decir, que dos elementos iguales tienen la misma imagen. Nuestra definición de $\overline{f}$ depende del representante de la clase escogida, por lo que debemos comprobar que al cambiar el representante no cambia la imagen de $\overline{f}$:

$$\forall a, b \in X \mid [a] = [b] \Rightarrow aRb \Rightarrow f(a) = f(b) \Rightarrow \overline{f}([a]) = \overline{f}([b])$$

Por tanto, tenemos que $\overline{f}$ es una aplicación. Comprobemos las tres propiedades que se enuncian:

1. Comprobemos que $Im(\overline{f}) = Im(f)$:

   $$Img(\overline{f}) = \{\overline{f}([a]) \mid [a] \in X/R\} = \{f(a) \mid [a] \in X/R\} = \{f(a) \mid a \in X\} = Img(f)$$

2. $\overline{f}$ es sobreyectiva $\iff Img(\overline{f}) = Y \iff Img(f) = Y \iff f$ es sobreyectiva.

3. Comprobemos que $\overline{f}$ es inyectiva $\iff$ $\forall a, b \in X \mid f(a) = f(b) \Rightarrow aRb$:

   $\Longrightarrow$) Sean $a, b \in X \mid f(a) = f(b) \Rightarrow \overline{f}([a]) = \overline{f}([b]) \Rightarrow [a] = [b] \Rightarrow aRb$

   $\Longleftarrow$) $\forall [a], [b] \in X/R \mid \overline{f}([a]) = \overline{f}([b]) \Rightarrow f(a) = f(b) \Rightarrow aRb \Rightarrow [a] = [b] \Rightarrow \overline{f}$ es inyectiva.

□

A la función $\overline{f}$ de la proposición anterior la llamaremos **aplicación inducida por f en el conjunto cociente**.

2. Anillos conmutativos

Definición 2.1 (Operación Binaria)**.** Sea A un conjunto no vacío, una **operación binaria** en A es una aplicación

$$* : A \times A \longrightarrow A$$

Dada dicha aplicación, para cada $(a, b) \in A \times A$, la imagen de ese par por dicha aplicación suele denotarse como $a * b$. Es decir:

$$*(a, b) =: a * b$$

Y se lee como el resultado de operar a con b mediante la operación $*$.

Ejemplo. Sea X un conjunto y $A = \mathcal{P}(X)$, entonces:

$$\cap : \mathcal{P}(X) \times \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$$
$$\cup : \mathcal{P}(X) \times \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$$

Son operaciones binarias en A.

Usaremos la notación aditiva o multiplicativa para las operaciones binarias:

- Notación aditiva: $+ : A \times A \longrightarrow A$ donde $a + b$ se leerá a más b.
- Notación multiplicativa: $\cdot : A \times A \longrightarrow A$ donde $a \cdot b$ se leerá a por b. En varias ocasiones, la notación multiplicativa será abreviada simplemente por yuxtaposición, entendiendo que $ab = a \cdot b$.

Definición 2.2 (Anillo Conmutativo, *Emmy Noether, 1921*)**.** Un **anillo conmutativo** es un conjunto no vacío A junto con dos operaciones, una notada aditivamente y otra multiplicativamente, de la siguiente forma:

$$+ : A \times A \longrightarrow A \qquad \cdot : A \times A \longrightarrow A$$

Tal que se verifica $\forall a, b, c \in A$:

1. Asociativa de la suma: $(a + b) + c = a + (b + c)$.
2. Conmutativa de la suma: $a + b = b + a$.
3. Existencia de un neutro de la suma (o cero): $\exists n \in A \mid a + n = a \quad \forall a \in A$.
4. Existencia de opuesto: $\forall a \in A \; \exists - a \in A \mid a + (-a) = n$.

5. Asociativa del producto: $(ab)c = a(bc)$.

6. Conmutativa del producto: $ab = ba$.

7. Existencia de un neutro del producto (o uno): $\exists d \in A \mid a \cdot d = a \quad \forall a \in A$.

8. Propiedad distributiva: $a(b + c) = ab + ac$.

Diremos que un conjunto no vacío A es simplemente un **anillo** si verifica todas las propiedades anteriores sin necesidad de verificar la 6.

Ejemplo. Algunos ejemplos de anillos conmutativos son:

1. $\mathbb{Z}$ es un anillo conmutativo con $+$ y $\cdot$, al igual que $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

   Notemos que $\mathbb{N}$ no lo es (no cumple 4).

2. Sea $A = \{f : [0,1] \longrightarrow \mathbb{R} \mid f \text{ es una aplicación}\}$ es anillo conmutativo con la suma y el producto definidos por $(\forall f, g \in A)$:

$$f + g : [0,1] \longrightarrow \mathbb{R} \mid (f+g)(x) = f(x) + g(x) \quad \forall x \in [0,1]$$
$$f \cdot g : [0,1] \longrightarrow \mathbb{R} \mid (f \cdot g)(x) = f(x)g(x) \quad \forall x \in [0,1]$$

   El cero es la aplicación $0 : [0,1] \longrightarrow \mathbb{R}$ definida por $0(x) = 0 \quad \forall x \in [0,1]$.

   El uno es la aplicación $1 : [0,1] \longrightarrow \mathbb{R}$ definida por $1(x) = 1 \quad \forall x \in [0,1]$.

   La aplicación opuesta de $f : [0,1] \longrightarrow \mathbb{R}$ es la aplicación $-f : [0,1] \longrightarrow \mathbb{R}$ definida por $(-f)(x) = -f(x) \quad \forall x \in [0,1]$.

3. Sea $n \geqslant 2$, entonces $M_n(\mathbb{R})$, conjunto de matrices cuadradas de orden n con entradas reales es un ejemplo de anillo no conmutativo[1] con la suma y el producto de matrices.

4. Otro ejemplo de anillo conmutativo es el conjunto $A = \{0\}$ con las operaciones:

$$\begin{array}{rcl} + : A \times A & \longrightarrow & A \\ (0,0) & \longmapsto & 0 + 0 = 0 \end{array}$$

$$\begin{array}{rcl} \cdot : A \times A & \longrightarrow & A \\ (0,0) & \longmapsto & 0 \cdot 0 = 0 \end{array}$$

   A este anillo lo llamaremos **anillo trivial**. Se trata del único anillo conmutativo que podemos formar con un conjunto unitario.

Propiedades

Deducidas de la definición de anillo conmutativo. Sea A un anillo conmutativo:

1. El cero y el 1 son únicos.

   Supongamos que $0, 0' \in A$ son dos ceros, luego $0 = 0 + 0' = 0'$.
   Supongamos que $1, 1' \in A$ son dos unos, luego $1 = 1 \cdot 1' = 1'$.

[1] Ya que si A y $B \in M_n(\mathbb{R})$, puede suceder que $A \cdot B \neq B \cdot A$.

2. $\forall a \in A$, $\exists_1 - a \in A \mid a + (-a) = 0$. (Podremos notar $a + (-a)$ como $a - a$).

   Supongamos que $-a, a' \in A$ son dos opuestos de a. Luego:

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

3. $\forall a \in A, -(-a) = a \ \wedge \ -0 = 0$.

$$0 + 0 = 0 \Longrightarrow -0 = 0$$
$$a + (-a) = 0 \Longrightarrow -(-a) = a$$

4. $\forall a \in A \ \ 0 \cdot a = 0$.

   Notemos que $0 \cdot a = (0 + 0)a = 0 \cdot a + 0 \cdot a$. Entonces:

$$0 \cdot a - 0 \cdot a = 0 = 0 \cdot a + 0 \cdot a - 0 \cdot a = 0 \cdot a \Longrightarrow 0 = 0 \cdot a$$

5. $\forall a, b, c \in A$, se cumple que:

   a) $(-a)b = -(ab) = a(-b)$. Esto es ya que:

$$0 = 0 \cdot b = (a - a)b = ab + (-a)b = 0 \Longrightarrow -(ab) = (-a)b$$

   b) $(-a)(-b) = ab$

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$$

   c) $(-1)a = -a$

   d) $(-1)(-1) = 1$

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

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

Como consecuencia, se verifica el siguiente lema:

Lema 2.1. *Sea A un anillo. Tenemos que:*

$$A \text{ es el anillo trivial } \Longleftrightarrow 0 = 1$$

Demostración. Procedemos mediante doble implicación:

$\Longrightarrow$) Si A es el anillo trivial, por definición tenemos que $0 = 1$.

$\Longleftarrow$) $\forall a \in A$, $a = a \cdot 1 = a \cdot 0 = 0 \Longrightarrow a = 0 \Longrightarrow A = \{0\}$.

□

2.1. Anillos de enteros módulo n

Definición 2.3. Sea $n \geqslant 2$, definimos sobre $\mathbb{Z}$ la siguiente relación binaria, que notaremos como R_n:

Dados $a, b \in \mathbb{Z}$, $aR_nb \iff \exists q \in \mathbb{Z} \mid a - b = qn$.

Lema 2.2. *Se verifica que R_n es una relación de equivalencia.*

Demostración. Comprobemos las tres condiciones para que una relación binaria sea de equivalencia:

- Reflexividad: $\forall a \in \mathbb{Z} \;\; a - a = 0 = qn$ con $q = 0 \in \mathbb{Z} \Longrightarrow aR_na$.
- Simetría: $\forall a, b \in \mathbb{Z} \mid bR_na$ se tiene que $\exists q \in \mathbb{Z}$ tal que $b - a = qn$. Por tanto, $a - b = -(b - a) = -qn$ con $-q \in \mathbb{Z} \Longrightarrow aR_nb$.
- Transitividad: $\forall a, b, c \in \mathbb{Z}$ tal que $aR_nb \;\wedge\; bR_nc$ se tiene que $\exists q, p \in \mathbb{Z}$ con $a-b = qn \wedge b-c = pn$. Entonces, $a-c = (a-b)+(b-c) = qn+pn = (q+p)n$, con $q + p \in \mathbb{Z} \Longrightarrow aR_nc$.

□

Para cada $n \geqslant 2$ consideramos el conjunto cociente de $\mathbb{Z}$ por R_n, notado a partir de ahora como $\mathbb{Z}_n$:

$$\mathbb{Z}_n = \mathbb{Z}/R_n = \{[a] \mid a \in \mathbb{Z}\}$$

donde para cada $a \in \mathbb{Z}$:

$$[a] = \{x \in \mathbb{Z} \mid xR_na\} = \{x \in \mathbb{Z} \mid x - a = qn, \;\; q \in \mathbb{Z}\} = \{a + qn \mid q \in \mathbb{Z}\}$$

Proposición 2.3. *Sea $n \geqslant 2$ y $a, a', b, b' \in \mathbb{Z} \mid aR_na' \;\wedge\; bR_nb'$. Entonces:*

$$(a + b)R_n(a' + b') \qquad (ab)R_n(a'b')$$

Demostración. Por la definición de dicha relación de equivalencia:

$$aR_na' \Longrightarrow \exists q \in \mathbb{Z} \mid a - a' = qn$$
$$bR_nb' \Longrightarrow \exists p \in \mathbb{Z} \mid b - b' = pn$$

Demostramos en primer lugar la suma:

$$(a + b) - (a' + b') = (a - a') + (b - b') = qn + pn = (q + p)n \overset{q+p\in\mathbb{Z}}{\Longrightarrow} (a + b)R_n(a' + b')$$

Respecto al producto:

$$ab-a'b' = ab+a'b-a'b-a'b' = (a-a')b+(b-b')a' = qnb+pna' = (qb+pa')n \overset{qb+pa'\in\mathbb{Z}}{\Longrightarrow} (ab)R_n(a'b')$$

□

Teorema 2.4 (Anillo de enteros/restos módulo n)**.** *Para cada $n \geqslant 2$, $\mathbb{Z}_n$ es un anillo conmutativo con operaciones suma y producto definidas por:*

$$[a] + [b] = [a + b] \qquad [a][b] = [ab], \qquad \forall a, b \in \mathbb{Z}$$

Dicho anillo lo denominaremos el ***anillo de enteros módulo*** *n, o también, el anillo de restos módulo n.*

Demostración. Por la Proposición 2.3, la suma y el producto no dependen del representante, por lo que están bien definidos.

- Las propiedades conmutativas, asociativas y distributiva son consecuencia inmediata de las propiedades de las operaciones en $\mathbb{Z}$.
- $[0]$ es el neutro para la suma.
- $[1]$ es el neutro para el producto.
- Dado $[a] \in \mathbb{Z}_n$, su opuesto es $-[a] = [-a] \in \mathbb{Z}_n$.

□

Teorema 2.5 (Algoritmo de la división de Euclides)**.** *Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces $\exists_1\ q, r \in \mathbb{Z}$ tal que:*

1. $a = bq + r$.
2. $0 \leqslant r < |b|$.

A q y a r se les llama cociente y resto de dividir a entre b, respectivamente.

Demostración. Supuesta la existencia de q y r, nos disponemos primero a mostrar su unicidad. Sean $q, q', r, r' \in \mathbb{Z} \mid a = bq + r,\ \ a = bq' + r', \quad 0 \leqslant r, r' < |b|$. Entonces:

$$bq + r = bq' + r' \Longrightarrow b(q - q') = r' - r$$

- Si $q = q'$: Entonces, se tiene que $r = r'$, por lo que queda demostrada la unicidad de q, r.
- Si $q \neq q'$: Tenemos que $|q - q'| > 0$. Además,

  $$|b|\ |q - q'| = |r' - r| \Longrightarrow |r' - r| > |b|$$

  en contradicción con que $0 \leqslant |r' - r| < |b|$ o, equivalentemente, $0 \leqslant r, r' < |b|$.

Por tanto, queda demostrado que $q = q',\ r = r'$.

Demostramos ahora la existencia, $\exists q, r \in \mathbb{Z} \mid a = bq + r\ \wedge\ 0 \leqslant r < |b|$. Sean $a, b \in \mathbb{Z} \mid a \geqslant 0\ \wedge\ b \geqslant 1$. Realizamos la siguiente distinción de casos:

- Si $a < b$:

  Entonces, considerando $q = 0$ y $r = a$, se tiene que:

  $$a = 0b + a \qquad 0 \leqslant a < |b| = b$$

- Si $a \geqslant b$:

  Sea $X = \{a - bq \mid q \in \mathbb{N}\} \cap \mathbb{N}$. Tenemos que $X \neq \emptyset$ por ser $a - b \in X$. Como $\emptyset \neq X \subseteq \mathbb{N}$, con $\mathbb{N}$ bien ordenado[2], X tiene mínimo. Sea $r = \min X$. Como

[2]Este teorema es materia de la asignatura de Cálculo I.

$r \in X \Longrightarrow r \geqslant 0 \ \wedge \ \exists q \in \mathbb{N} \mid r = a - bq \Longrightarrow a = bq + r$. Falta que $r < b$:

Por reducción al absurdo, supongamos que $r \geqslant b$ y consideramos $r' = r - b \geqslant 0$.

$$r' = r - b = a - bq - b = a - b(q+1) \overset{r' \geqslant 0}{\Longrightarrow} r' \in X \ \wedge \ r' < r$$

Contradicción con que r era el mínimo de X. Por tanto, se tiene que $r < b$.

Ejemplo. Consideramos $a = 3254, \ b = 17$. Tenemos que la división es:

$$\begin{array}{rr|l} 3\ 2\ 5\ 4 & & 1\ 7 \\ \cline{3-3} 1\ 5\ 5 & & 1\ 9\ 1 \\ \quad 2\ 4 & & \\ \quad\ \ 7 & & \end{array}$$

Por tanto, $3254 = 17 \cdot 191 + 7$. Es decir, $q = 191, \ r = 7$.

- Dividir $-a$ entre b:

  Dividimos a entre b y obtenemos $q, r \in \mathbb{Z} \mid a = bq + r \ \wedge \ 0 \leqslant r < |b|$.

  - Si $r = 0 \Longrightarrow a = bq \Longrightarrow -a = -bq = b(-q)$.
  - Si $r \neq 0$, como $a = bq + r$, se tiene que:

    $$-a = -bq - r = -bq - b + b - r = b(-q-1) + b - r$$

    Por lo que el cociente es $-q - 1$ y el resto es $b - r$, siendo $0 \leqslant b - r < |b|$.

  Ejemplo. Sabemos que $3254 = 17 \cdot 191 + 7$. Por tanto, $-3254 \div 17$ tiene por cociente -192 y resto $17 - 7 = 10$. Por tanto, $-3254 = 17 \cdot -192 + 10$.

- Dividir a entre $-b$:

  Dividimos a entre b y obtenemos $q, r \in \mathbb{Z} \mid a = bq + r \ \wedge \ 0 \leqslant r < |b|$. Tenemos que $a = (-b)(-q) + r$, por lo que el cociente es $-q$ y el resto es r.

  Ejemplo. Sabemos que $3254 = 17 \cdot 191 + 7$. Por tanto, $3254 \div -17$ tiene por cociente -191 y resto 7. Por tanto, $3254 = -17 \cdot -191 + 7$.

- Dividir $-a$ entre $-b$:

  Dividimos a entre b y obtenemos $q, r \in \mathbb{Z} \mid a = bq + r \ \wedge \ 0 \leqslant r < |b|$.

  - Si $r = 0 \Longrightarrow a = bq \Longrightarrow -a = -bq = (-b)q$.
  - Si $r \neq 0$, como $a = bq + r$, se tiene que:

    $$-a = -bq - r = -bq - b + b - r = (-b)(q+1) + b - r$$

    Por lo que el cociente es $q + 1$ y el resto es $b - r$, siendo $0 \leqslant b - r < |b|$.

  Ejemplo. Sabemos que $3254 = 17 \cdot 191 + 7$. Por tanto, $(-3254) \div (-17)$ tiene por cociente 192 y resto $17 - 7 = 10$. Por tanto, $-3254 = -17 \cdot 192 + 10$.

□

Teorema 2.6 (Estructura del anillo de enteros módulo n)**.** *Sea $n \geqslant 2$:*

$$\mathbb{Z}_n = \mathbb{Z}/R_n = \{[0], [1], \ldots, [n-1]\}$$

Demostración. Sabemos que $\{[0], [1], \ldots, [n-1]\} \subseteq \mathbb{Z}_n$.

Sea $a \in \mathbb{Z}$. Consideramos $[a] \in \mathbb{Z}_n$ y dividimos a entre n. Por el teorema anterior, $\exists\, q, r \in \mathbb{Z} \mid a = nq + r \ \wedge \ 0 \leqslant r < n$ cumpliendo que:

$$a - r = nq \Longrightarrow aR_n r \Longrightarrow [a] = [r]$$

Por tanto, como $0 \leqslant r < n \Longleftrightarrow 0 \leqslant r \leqslant n-1$, tenemos que

$$[a] = [r] \in \{[0], [1], \ldots, [n-1]\} \Longrightarrow \mathbb{Z}_n \subseteq \{[0], [1], \ldots, [n-1]\}$$

Por tanto, se tiene la igualdad por la doble inclusión. □

Notación. Si para cada $a \in \mathbb{Z}$ notamos por $R(a; n)$ al resto r de dividir a entre n, entonces:

$$[a] = [R(a; n)]$$

Por ejemplo, en $\mathbb{Z}_3$, tenemos que $[11] = [2]$. Notemos que:

$$\begin{gathered}[a] + [b] = [R(a+b; n)] \\ [a] \cdot [b] = [R(ab; n)] \\ -[a] = [-a] = [R(-a; n)] \overset{(*)}{=} [n-a]\end{gathered}$$

donde la igualdad $(*)$ solo es cierta si $0 \leqslant a \leqslant n-1$.

Notación. A partir de ahora, se omitirán los corchetes (por comodidad) a la hora de representar las clases de equivalencia, por lo que tendremos que $\mathbb{Z}_n$ es un anillo conmutativo de la forma (con $n \geqslant 2$):

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

Teniendo en cuenta que, para $a, b \in \mathbb{Z}_n$:

$$\begin{aligned} a + b &= R(a+b; n) \\ ab &= R(ab; n) \\ -a &= R(-a, n) \end{aligned}$$

Ejemplo. En $\mathbb{Z}_8 = \{0, 1, \ldots, 7\}$:

$$3 \cdot 7 = 5 \qquad 3 \cdot 3 = 1 \qquad -5 = 3 \qquad 2 \cdot 4 = 0$$

2.2. Anillos de enteros cuadráticos y anillos de racionales cuadráticos

Definición 2.4 (Subanillo)**.** Sea A un anillo conmutativo. Un subconjunto $B \subseteq A$, $B \neq \emptyset$ diremos que es un **subanillo** de A si verifica:

1. $\forall a, b \in B \;\; a + b, ab \in B$. Cerrado para suma y producto.
2. $0, 1 \in B$. Contiene al 1 y al 0.
3. $\forall a \in B. \;\; -a \in B$. Cerrado para opuestos.

Notemos que si B es un subanillo de A, tenemos que $(B, +, \cdot)$ es un anillo conmutativo.

Notación. Sea $a \in \mathbb{R}^+$, $\exists b, c \in \mathbb{R} \mid b^2 = c^2 = a$ con $b \in \mathbb{R}^+$ y $c \in \mathbb{R}^-$.
Notaremos: $\sqrt{a} = b \;\wedge\; -\sqrt{a} = c$.

Notación. No existe ningún real cuyo cuadrado sea $-a$, con $a \in \mathbb{R}^+$. Sabemos de la existencia de dos números complejos. Uno es $i\sqrt{a}$ y otro es su opuesto, $-i\sqrt{a}$.
A $i\sqrt{a}$ lo notaremos como $\sqrt{-a}$.

Proposición 2.7 (Anillo de enteros cuadráticos)**.** *Sea $n \in \mathbb{Z} \mid \sqrt{n} \notin \mathbb{Z}$. Consideramos el siguiente subconjunto de $\mathbb{C}$:*

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

Notemos que si $n > 0 \Longrightarrow \mathbb{Z}[\sqrt{n}] \subseteq \mathbb{R}$.

Se verifica que $\mathbb{Z}[\sqrt{n}]$ es subanillo de $\mathbb{C}$, que llamaremos ***el anillo de enteros cuadráticos*** *definido por n.*

Demostración. Sean $\alpha, \beta \in \mathbb{Z}[\sqrt{n}] \Longrightarrow \exists a, b, a', b' \in \mathbb{Z} \mid \alpha = a + b\sqrt{n} \wedge \beta = a' + b'\sqrt{n}$.
Veamos en primer lugar que es cerrado para la suma:

$$\alpha + \beta = (a + b\sqrt{n}) + (a' + b'\sqrt{n}) = (a + a') + (b + b')\sqrt{n}$$
$$a + a' \in \mathbb{Z} \;\wedge\; b + b' \in \mathbb{Z} \Longrightarrow \alpha + \beta \in \mathbb{Z}[\sqrt{n}]$$

Veamos ahora si es cerrado para el producto:

$$\alpha\beta = (a + b\sqrt{n})(a' + b'\sqrt{n}) = aa' + ab'\sqrt{n} + ba'\sqrt{n} + bb'n = (aa' + bb'n) + (ab' + ba')\sqrt{n}$$
$$aa' + bb'n \in \mathbb{Z} \;\wedge\; ab' + ba' \in \mathbb{Z} \Longrightarrow \alpha\beta \in \mathbb{Z}[\sqrt{n}]$$

Tenemos que $\mathbb{Z}[\sqrt{n}]$ es cerrado para operaciones. Veamos si contiene al 1 y al 0.

$$0 = 0 + 0\sqrt{n} \qquad 1 = 1 + 0\sqrt{n}$$

Como $0, 1 \in \mathbb{Z}$, tenemos que $0, 1 \in \mathbb{Z}[\sqrt{n}]$. Comprobemos ahora que es cerrado para opuestos:

$$\alpha = a + b\sqrt{n} \Longrightarrow -\alpha = -a - b\sqrt{n} \qquad -a, -b \in \mathbb{Z} \Longrightarrow -\alpha \in \mathbb{Z}[\sqrt{n}]$$

Luego $\mathbb{Z}[\sqrt{n}]$ es cerrado para opuestos. Por tanto, queda demostrado que $\mathbb{Z}[\sqrt{n}]$ es un subanillo de $\mathbb{C}$ □

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

Ejemplo. Algunos ejemplos de anillos de enteros cuadráticos son:

1. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.
2. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

   Este segundo anillo se denomina el anillo de enteros de Gauss. Notemos que no coincide con $\mathbb{C}$, ya que en los complejos los coeficientes a, b pueden ser reales, mientras que en este caso nos limitamos a enteros.

Proposición 2.8 (Anillo de racionales cuadráticos)**.** *Sea $n \in \mathbb{Z} \mid \sqrt{n} \notin \mathbb{Z}$. Consideramos el siguiente subconjunto de $\mathbb{C}$:*

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

Se verifica que $\mathbb{Q}[\sqrt{n}]$ es un subanillo de $\mathbb{C}$, que llamaremos ***el anillo de racionales cuadráticos*** *definido por n.*

Demostración. Análoga a la de la Proposición 2.7, basándose en que $\mathbb{Q}$ es cerrado para operaciones y opuestos y que contiene al 1 y al 0. □

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

Definición 2.5 (Unidad)**.** Sea A un anillo conmutativo. Un elemento $u \in A$ diremos que u es una **unidad** (o que es invertible) si existe $v \in A \mid uv = 1$.

En tal caso, dicho v es único, puesto que si $v' \in A \mid uv' = 1$, entonces:

$$v' = v' \cdot 1 = (v'u)v = 1 \cdot v = v$$

A este elemento único v lo llamaremos **inverso de** u y lo notaremos por u^{-1}.

En cualquier anillo, el 1 y el -1 son unidades, con $1^{-1} = 1 \ \wedge \ (-1)^{-1} = -1$.

No todos los elementos de un anillo conmutativo son unidades. Si el anillo es no trivial; el 0, por ejemplo, no es una unidad[3].

Notación. Al conjunto de unidades de un anillo A conmutativo lo notaremos $\mathcal{U}(A)$:

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

Ejemplo. Algunos ejemplos de unidades en anillos ya conocidos son:

$$\begin{aligned} \mathcal{U}(\mathbb{Z}) &= \{-1, 1\} \\ \mathcal{U}(\mathbb{Z}_2) &= \{1\} \\ \mathcal{U}(\mathbb{Z}_3) &= \{1, 2\} \\ \mathcal{U}(\mathbb{Z}_4) &= \{1, 3\} \\ \mathcal{U}(\mathbb{Z}_5) &= \{1, 2, 3, 4\} \end{aligned}$$

[3]Ya que $a \cdot 0 = 0 \neq 1 \ \forall a \in A$.

Definición 2.6 (Cuerpo)**.** Un anillo conmutativo K diremos que es un **cuerpo** si K es no trivial y todos los elementos no nulos de K son unidades, es decir:

$$\mathcal{U}(K) = K \setminus \{0\}$$

Ejemplo. Ejemplos de cuerpos son: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$. Veamos el caso de los números complejos, $\mathbb{C}$:

$$\forall \alpha = a + bi \in \mathbb{C} \mid \alpha \neq 0 \qquad \frac{1}{\alpha} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i$$

Definición 2.7 (Conjugado)**.** Sea $\alpha = a + b\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$ $(n \geqslant 2 \ \sqrt{n} \notin \mathbb{Z})$. Definimos el **conjugado de** α, denotado por $\overline{\alpha}$, como el elemento:

$$\overline{\alpha} = a - b\sqrt{n}$$

En el caso de $\mathbb{Z}[\sqrt{n}]$, al ser este subanillo de los racionales cuadráticos, se define el conjugado de forma análoga.

Algunas propiedades del conjugado de los racionales cuadráticos son, tomando $\alpha = a + b\sqrt{n}, \quad \beta = c + d\sqrt{n} \quad \in \mathbb{Q}[\sqrt{n}]$:

1. $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta} \qquad \forall \alpha, \beta \in \mathbb{Q}[\sqrt{n}]$.

$$\overline{\alpha + \beta} = \overline{(a + c) + (b + d)\sqrt{n}} = (a + c) - (b + d)\sqrt{n}$$
$$\overline{\alpha} + \overline{\beta} = a - b\sqrt{n} + c - d\sqrt{n} = (a + c) - (b + d)\sqrt{n}$$

2. $\overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta} \qquad \forall \alpha, \beta \in \mathbb{Q}[\sqrt{n}]$.

$$\overline{\alpha\beta} = \overline{(ac + bdn) + (bc + da)\sqrt{n}} = (ac + bdn) - (bc + da)\sqrt{n}$$
$$\overline{\alpha} \cdot \overline{\beta} = (a - b\sqrt{n})(c - d\sqrt{n}) = (ac + bdn) - (bc + da)\sqrt{n}$$

3. $\overline{\overline{\alpha}} = \alpha \qquad \forall \alpha \in \mathbb{Q}[\sqrt{n}]$.

$$\overline{\overline{\alpha}} = \overline{\overline{a + b\sqrt{n}}} = \overline{a - b\sqrt{n}} = a + b\sqrt{n} = \alpha$$

Definición 2.8 (Norma)**.** Dado $\alpha = a + b\sqrt{n} \quad \in \mathbb{Q}[\sqrt{n}]$, definimos la **norma de** α, notada $N(\alpha)$, por:

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

Respecto a la norma, se verifica que, dados $\alpha, \beta \in \mathbb{Q}[\sqrt{n}]$, con $\alpha = a + b\sqrt{n}$, se tiene que:

1. $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta) \qquad \forall \alpha, \beta \in \mathbb{Q}[\sqrt{n}]$

$$N(\alpha \cdot \beta) = (\alpha \cdot \beta) \cdot \overline{\alpha \cdot \beta} = (\alpha \cdot \beta) \cdot (\overline{\alpha} \cdot \overline{\beta}) = (\alpha \cdot \overline{\alpha}) \cdot (\beta \cdot \overline{\beta}) = N(\alpha) \cdot N(\beta)$$

2. $N(\alpha) = 0 \iff \alpha = 0$

$\Longrightarrow$) $\alpha = 0 \Longleftrightarrow \alpha = 0 + 0\sqrt{n} \Longrightarrow N(\alpha) = 0$

$\Longleftarrow$) Tenemos que $N(\alpha) = 0 \Longleftrightarrow \alpha \cdot \overline{\alpha} = 0$ Por tanto,

- Si $\overline{\alpha} = 0 \Longrightarrow \overline{\alpha} = a - b\sqrt{n} = 0 \Longleftrightarrow a = 0 \ \wedge \ b = 0$. Por tanto, $\alpha = a + b\sqrt{n} = 0$
- Si $\alpha = 0$, se tiene lo que queríamos demostrar.

Proposición 2.9. *$\mathbb{Q}[\sqrt{n}]$ es un cuerpo (con $n \in \mathbb{Z} \mid \sqrt{n} \notin \mathbb{Z}$).*

Demostración. Hemos de demostrar que todo elemento no nulo de $\mathbb{Q}[\sqrt{n}]$ es una unidad. Consideramos $\alpha \in \mathbb{Q}[\sqrt{n}]$, $\alpha \neq 0$. veamos si α es una unidad.

En primer lugar, por lo visto anteriormente, como $\alpha \neq 0$ tenemos que $N(\alpha) \neq 0$. Consideramos ahora el siguiente elemento, $\beta = \dfrac{\overline{\alpha}}{N(\alpha)} \in \mathbb{Q}[\sqrt{n}]$. Veamos que:

$$\alpha \cdot \beta = \alpha \cdot \frac{\overline{\alpha}}{N(\alpha)} = \frac{N(\alpha)}{N(\alpha)} = 1$$

Por lo que tenemos que $\alpha = a + b\sqrt{n} \in \mathcal{U}(\mathbb{Q}[\sqrt{n}])$, siendo:

$$\alpha^{-1} = \beta = \frac{\overline{\alpha}}{N(\alpha)} = \frac{a}{N(\alpha)} - \frac{b}{N(\alpha)}\sqrt{n}$$

□

Ejemplo. En $\mathbb{Q}[\sqrt{2}]$, consideramos $\alpha = 3 - \sqrt{2}$. Veamos que es una unidad.

Tenemos que $N(\alpha) = 3^2 - 2 = 7$, por lo que:

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

Notemos que $\alpha \in \mathbb{Z}[\sqrt{n}] \subsetneq \mathbb{Q}[\sqrt{n}]$ mientras que $\alpha^{-1} \notin \mathbb{Z}[\sqrt{n}]$, $\alpha^{-1} \in \mathbb{Q}[\sqrt{n}]$

Proposición 2.10. *Sea $\alpha = a + b\sqrt{n} \quad \in \mathbb{Z}[\sqrt{n}]$*

$$\alpha \in \mathcal{U}(\mathbb{Z}[\sqrt{n}]) \Longleftrightarrow N(\alpha) = \pm 1$$

Demostración. Demostramos mediante doble implicación:

$\Longrightarrow$) Sea $\alpha \in \mathcal{U}(\mathbb{Z}[\sqrt{n}]) \Longrightarrow \exists \alpha^{-1} \in \mathbb{Z}[\sqrt{n}] \mid \alpha \cdot \alpha^{-1} = 1$. Tenemos que:

$$N(\alpha) \cdot N(\alpha^{-1}) = N(\alpha \cdot \alpha^{-1}) = N(1) = 1$$

Tenemos por tanto que $N(\alpha), N(\alpha^{-1}) \in \mathbb{Z} \mid N(\alpha) \cdot N(\alpha^{-1}) = 1$. Por tanto,

$$N(\alpha) \in \mathcal{U}(\mathbb{Z}) = \{-1, 1\} \Longrightarrow N(\alpha) = \pm 1$$

$\Longleftarrow$) Sea $\alpha \in \mathbb{Z}[\sqrt{n}] \mid N(\alpha) = \pm 1$:

- $N(\alpha) = 1 \Longrightarrow \alpha \cdot \overline{\alpha} = 1 \Longrightarrow \alpha \in \mathcal{U}(\mathbb{Z}[\sqrt{n}])$ con $\alpha^{-1} = \overline{\alpha}$.
- $N(\alpha) = -1 \Longrightarrow -N(\alpha) = -\alpha \cdot \overline{\alpha} = 1 \Longrightarrow \alpha \in \mathcal{U}(\mathbb{Z}[\sqrt{n}])$ con $\alpha^{-1} = -\overline{\alpha}$.

□

Ejemplo. En el anillo de los enteros de Gauss, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, calcular las unidades. Tenemos que $N(a + bi) = a^2 + b^2$, por lo que, usando la proposición anterior:

$$\alpha \in \mathcal{U}(\mathbb{Z}[i]) \iff a^2+b^2 = 1 \iff \left\{ \begin{array}{ccc} a^2 = 1 & & a^2 = 0 \\ \wedge & \vee & \wedge \\ b^2 = 0 & & b^2 = 1 \end{array} \right\} \iff \left\{ \begin{array}{ccc} a = \pm 1 & & a = 0 \\ \wedge & \vee & \wedge \\ b = 0 & & b = \pm 1 \end{array} \right\}$$

Por tanto, tenemos que $U[\mathbb{Z}[i]] = \{-1, 1, -i, i\}$.

Ejemplo. Sea $n \geqslant 2$ y $\mathbb{Z}[\sqrt{-n}] = \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}\}$. Calcular las unidades de dicho anillo.

Sea $\alpha = a + b\sqrt{-n} \quad \in \mathbb{Z}[\sqrt{-n}]$. Tenemos que $N(\alpha) = a^2 + nb^2 \geqslant 0$. Por tanto,

$$\alpha \in \mathcal{U}(\mathbb{Z}[\sqrt{-n}]) \iff N(\alpha) = a^2 + nb^2 = 1 \iff a = \pm 1 \ \wedge \ b = 0$$

Luego $\mathcal{U}(\mathbb{Z}[\sqrt{-n}]) = \{-1, 1\}$.

Ejemplo. Consideramos $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Calcular las unidades de dicho anillo.

Sea $\alpha = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Tenemos que $N(a + b\sqrt{2}) = a^2 - 2b^2$. Por tanto,

$$\alpha \ \in \mathcal{U}(\mathbb{Z}[\sqrt{2}]) \iff a^2 - 2b^2 = \pm 1$$

Por lo que el conjunto de las unidades de $\mathbb{Z}[\sqrt{2}]$ es infinito:

$$\{1 + \sqrt{2}, -1, 1, 3 + 2\sqrt{2}\} \subsetneq \mathcal{U}(\mathbb{Z}[\sqrt{2}])$$

Se verifica que[4]:

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

2.3. Sumas y productos generalizados

Lo que vamos a proceder a ver en este tema es de gran importancia. A pesar de que para el alumno parezca trivial, permite trabajar simultáneamente con todo tipo de anillos conmutativos junto con los enteros. Hemos de pensar que un anillo conmutativo A no se limita a los conjuntos a los que el alumno está acostumbrado, como pueden ser los enteros.

Definición 2.9. Sea A un anillo conmutativo y sea $n \in \mathbb{N} \mid n \geqslant 1$. Sea $(a_1, a_2, \ldots, a_n) \in A^n$. Podemos definir la suma y el producto de n elementos de forma inductiva:

$$\sum_{i=1}^{n} a_i = \left\{ \begin{array}{ll} a_1 & \text{si } n = 1 \\ \sum\limits_{i=1}^{n-1} a_i + a_n & \text{si } n > 1 \end{array} \right.$$

$$\prod_{i=1}^{n} a_i = \left\{ \begin{array}{ll} a_1 & \text{si } n = 1 \\ \left(\prod\limits_{i=1}^{n-1} a_i\right) \cdot a_n & \text{si } n > 1 \end{array} \right.$$

[4]La resolución de dicha ecuación no entra en el contenido de este curso. Se conoce como Ecuación de Pell.

Proposición 2.11 (Propiedad asociativa generalizada)**.** *Sea A un anillo conmutativo, y sean $m, n \in \mathbb{N}$, $m, n \geqslant 1$. Sea $(a_1, a_2, \ldots, a_m, a_{m+1}, \ldots, a_{m+n}) \in A^{m+n}$. Se verifica que:*

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

$$\prod_{i=1}^{m+n} a_i = \left(\prod_{i=1}^{m} a_i\right) \cdot \left(\prod_{i=m+1}^{m+n} a_i\right)$$

Demostración. Demostramos para la suma. Para ello, fijamos el valor de m y realizamos inducción sobre n:

- Para $n = 1$: aplicamos 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 n, lo probamos para $n+1$:

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

Para el producto se realiza de una forma análoga. □

Notación. A veces, escribiremos:

$$\sum_{i=1}^{n} a_i =: a_1 + a_2 + \ldots + a_n$$

$$\prod_{i=1}^{n} a_i =: a_1 \cdot a_2 \cdot \ldots \cdot a_n$$

Proposición 2.12 (Propiedad distributiva generalizada)**.** *Sea A un anillo conmutativo, y sean $m, n \geqslant 1$ y consideramos $(a_1, a_2, \ldots, a_m) \in A^m$, $(b_1, b_2, \ldots, b_n) \in A^n$. Se verifica que:*

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$

Demostración. Demostramos mediante inducción en m:

- Para $m = 1$: Hacemos inducción en n:
  - Para $n = 1$, es obvio que $a_1 b_1 = a_1 b_1$.

- Supuesto cierto para un $n-1$, lo comprobamos para n:

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

- Supuesto cierto para un $m-1$, lo comprobamos para m:

$$\left(\sum_{i=1}^{m} a_i \right) \left(\sum_{j=1}^{n} b_j \right) = \left(\sum_{i=1}^{m-1} a_i + a_m \right) \left(\sum_{j=1}^{n} b_j \right) = \left(\sum_{i=1}^{m-1} a_i \right) \left(\sum_{j=1}^{n} b_j \right) + a_m \left(\sum_{j=1}^{n} b_j \right) =$$
$$= \left(\sum_{i=1}^{m-1} \sum_{j=1}^{n} a_i b_j \right) + \sum_{j=1}^{n} a_m b_j = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j$$

□

En el caso de tener una lista ($n \in \mathbb{N}$) $(a_1, a_2, \ldots, a_n) \in A^n$ en la que todos sus elementos son iguales:

$$a_1 = a_2 = \ldots = a_n = a$$

Tenemos que:

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n = n \cdot a$$
$$\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdot \ldots \cdot a_n = a^n$$

Con el convenio de que si $n = 0$, entonces: $\sum_{i=1}^{0} a_i = 0 \cdot a = 0$ y $\prod_{i=1}^{0} a_i = a^0 = 1$.

Proposición 2.13. *Sea A un anillo conmutativo y $n, m \in \mathbb{N}$, $a, b \in A$. Se verifica:*

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. $(a-b)(a+b) = a^2 - b^2$

Demostración.

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

$$(m+n)a = \sum_{i=1}^{m+n} a = \sum_{i=1}^{m} a + \sum_{i=m+1}^{m+n} a = ma + na$$

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

   Realizamos inducción sobre n:

   - Para $n = 0, 1$: $0 = 0$ y $a + b = a + b$, Cierto.
   - Cierto para n, lo probamos para $n + 1$:

$$(n+1)(a+b) = n(a+b)+a+b = na+nb+a+b = na+a+nb+b = (n+1)a+(n+1)b$$

3. $m(na) = (mn)a$ Realizamos inducción sobre m:

   - Para $m = 0, 1$: $0 = 0$ y $na = na$, Cierto.
   - Cierto para m, lo probamos para $m + 1$:

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

4. $(ma)(nb) = (mn)(ab)$

$$(ma)(nb) = \left(\sum_{i=1}^{m} a\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j = (mn)(ab)$$

5. $a^n a^m = a^{n+m}$

$$a^n a^m = \prod_{i=1}^{n} a + \prod_{i=m+1}^{n+m} a = \prod_{i=1}^{n+m} a = a^{n+m}$$

6. $(ab)^n = a^n b^n$

   Realizamos inducción sobre n:

   - Para $n = 0, 1$: $1 = 1$ y $ab = ab$, Cierto.
   - Cierto para n, lo probamos para $n + 1$:

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

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

   Realizamos inducción sobre n:

   - Para $n = 0, 1$: $1 = 1$ y $a^m = a^m$, Cierto.
   - Cierto para n, lo probamos para $n + 1$:

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

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

   Recordamos la definición de número combinatorio:

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

   Y tenemos en cuenta que:

$$\binom{n}{j} + \binom{n}{j-1} = \frac{n!}{j!(n-j)!} + \frac{n!}{(j-1)!(n-j+1)!} =$$

$$= \frac{n!(n-j)!(j-1)!(n-j+1+j)}{j!(n-j)!(j-1)!(n-j+1)!} = \frac{n!(n+1)}{j!(n-j+1)!} = \binom{n+1}{j}$$

   Para hacer la demostración, realizamos inducción sobre n:

   - Para $n = 1$:

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

   - Supuesto cierto para un n, lo probamos para $n+1$:

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

9. $(a-b)(a+b) = a^2 - b^2$

$$(a-b)(a+b) = a^2 - b^2 + ab - ab = a^2 - b^2$$

□

Proposición 2.14 (Cardinalidad del conjunto partes de un conjunto)**.** *Dado un conjunto $X \mid |X| = n \in \mathbb{N}$. Se verifica que:*

$$|\mathcal{P}(X)| = 2^n$$

Demostración. El conjunto $\mathcal{P}(X)$ consiste en el conjunto $\emptyset$, los n conjuntos de un sólo elemento de X, los $\binom{n}{2}$ subconjuntos de X de dos elementos, …, los $\binom{n}{i}$ subconjuntos de i elementos de X, …, y del conjunto X. De esta forma, tenemos que:

$$|\mathcal{P}(X)| = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{i} + \dots + \binom{n}{n} = (1+1)^n = 2^n$$

□

Proposición 2.15. *Sea $n \geqslant 1$, $(a_1, a_2, \ldots, a_n) \in A^n$. Entonces:*

$$-\left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} -a_i$$

Además, si $a_1, a_2, \ldots, a_n \in \mathcal{U}(A) \Longrightarrow \prod_{i=1}^{n} a_i \in \mathcal{U}(A)$, con:

$$\left(\prod_{i=1}^{n} a_i\right)^{-1} = \prod_{i=1}^{n} a_i^{-1}$$

Demostración. Demostramos simultáneamente mediante inducción en n:

- Para $n = 1$: Por definición, es cierto.
- Supuesto cierto para $n-1$, lo probamos para n:

$$\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} -a_i = \sum_{i=1}^{n-1} a_i + an + \sum_{i=1}^{n-1} -a_i - an = \sum_{i=1}^{n-1} a_i + \sum_{i=1}^{n-1} -a_i = 0$$

$$\left(\prod_{i=1}^{n} a_i\right)\left(\prod_{i=1}^{n} a_i^{-1}\right) = \left(\prod_{i=1}^{n-1} a_i\right) a_n \left(\prod_{i=1}^{n-1} a_i^{-1}\right) a_n^{-1} = \left(\prod_{i=1}^{n-1} a_i\right)\left(\prod_{i=1}^{n-1} a_i^{-1}\right) = 1$$

□

En el caso de tener una lista ($n \in \mathbb{N}$) $(a_1, a_2, \ldots, a_n) \in A^n$ en la que todos sus elementos son iguales:

$$a_1 = a_2 = \ldots = a_n = a$$

Tenemos que:

$$-(na) := (-n)a = -\left(\sum_{i=1}^{n} a\right) = \left(\sum_{i=1}^{n} -a\right) = n(-a) =: -na$$

Y podemos definir, si $a \in \mathcal{U}(A)$:

$$a^{-n} := (a^n)^{-1} = (a^{-1})^n$$

Proposición 2.16. *Sean $m, n \in \mathbb{Z}$, $a, b \in A$, $u, v \in \mathcal{U}(A)$. Se verifican:*

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

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

Demostración. Tan solo demostramos los casos en los que intervengan enteros negativos, ya que en caso contrario está demostrado en la proposición 2.13. Consideramos $m, n > 0$, y demostraremos por tanto para uno de los dos negativos ($-n$, sin perder generalidad), y ambos negativos.

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

   Demostramos en primer lugar si solo uno de los dos enteros es negativo. Trabajemos por tanto con $-n$:

   - Si $m \geqslant n$, definimos $k = m - n \geqslant 0$. Entonces:

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

   - Si $m < n$, definimos $k = n - m \geqslant 0$. Entonces:

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

   Demostramos ahora con ambos negativos:

   $$(-m-n)a = [-(m+n)a] = -[(m+n)a] = -(ma+na) = -ma - na$$

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

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

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

   Demostramos en primer lugar si solo uno de los dos enteros es negativo. Trabajemos por tanto con $-n$:

   $$(-n)(ma) = -[n(ma)] = -[(mn)a] = (-mn)a$$

   Demostramos ahora con ambos negativos:

   $$(-n)[(-m)a] = -[n(-(ma))] = (mn)a = [(-n)(-m)a]$$

4. $(na)(mb) = (nm)(ab)$

   Demostramos en primer lugar si solo uno de los dos enteros es negativo. Trabajemos por tanto con $-n$:

   $$(-na)(mb) = -[(na)(mb)] = -[(nm)(ab)] = -(nm)(ab) = [(-n)m](ab)$$

   Demostramos ahora con ambos negativos:

   $$(-na)(-mb) = (na)(mb) = (nm)(ab) = [(-n)(-m)](ab)$$

5. $u^m u^n = u^{m+n}$

   Demostramos en primer lugar si solo uno de los dos enteros es negativo. Trabajemos por tanto con $-n$:

- Si $m \geqslant n$, definimos $k = m - n \geqslant 0$. Entonces:

$$u^m u^{-n} = u^{n+k} u^{-n} = u^k u^n u^{-n} = u^k \cdot 1 = u^k = u^{m-n}$$

- Si $m < n$, definimos $k = n - m \geqslant 0$. Entonces:

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

Demostramos ahora con ambos negativos:

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

6. $(uv)^n = u^n v^n$

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

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

Demostramos en primer lugar si solo uno de los dos enteros es negativo. Trabajemos por tanto con $-n$:

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

Demostramos ahora con ambos negativos:

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

□

2.4. Homomorfismos de anillos

Definición 2.10 (Homomorfismo)**.** Un **homomorfismo de anillos de** A **en** A', siendo A, A' anillos conmutativos, es una aplicación $\phi : A \longrightarrow A'$ que verifica:

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$
3. $\phi(1) = 1 \in A'$

Ejemplo. Algunos ejemplos de homomorfismos son:

1. Si A es un anillo, la aplicación identidad

$$\begin{array}{rccc} id_A : & A & \longrightarrow & A \\ & a & \longmapsto & a \end{array}$$

es un homomorfismo de anillos.

2. Si B es un subanillo de A, la aplicación inclusión

$$\begin{array}{rcl} i : B & \longrightarrow & A \\ b & \longmapsto & b \end{array}$$

es un homomorfismo de anillos.

3. $\forall n \geqslant 1$, la **proyección canónica**

$$\begin{array}{rcl} p : \mathbb{Z} & \longrightarrow & \mathbb{Z}_n \\ a & \longmapsto & [a] \end{array}$$

es un homomorfismo de anillos. Demostramos esta:

a) $p(a+b) = [a+b] = [a] + [b] = p(a) + p(b)$.

b) $p(ab) = [ab] = [a][b] = p(a)p(b)$.

c) $p(1) = [1]$.

Proposición 2.17. *Sean A, A' anillos conmutativos, $\phi : A \longrightarrow A'$ un homomorfismo de anillos y $a \in A$, $u \in \mathcal{U}(A)$, $n \in \mathbb{Z}$. Se verifican:*

1. $\phi\left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} \phi(a_i)$
2. $\phi\left(\prod_{i=1}^{n} a_i\right) = \prod_{i=1}^{n} \phi(a_i)$
3. $\phi(0) = 0$
4. $\phi(-a) = -\phi(a)$
5. $\phi(na) = n\phi(a)$
6. $\phi(a^n) = (\phi(a))^n$ *si* $n \in \mathbb{N}$
7. $\phi(u) \in \mathcal{U}(A') \ \wedge \ \phi(u^{-1}) = (\phi(u))^{-1}$
8. $\phi(u^n) = (\phi(u))^n$

Demostración.

1. $\phi\left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} \phi(a_i)$

   Realizamos inducción en n:

   - Para $n = 1$: $\phi(a_1) = \phi(a_1)$, Cierto.
   - Supuesto cierto para $n-1$, lo probamos para n:

$$\phi\left(\sum_{i=1}^{n} a_i\right) = \phi\left(\sum_{i=1}^{n-1} a_i\right) + \phi(a_n) = \sum_{i=1}^{n-1} \phi(a_i) + \phi(a_n) = \sum_{i=1}^{n} \phi(a_i)$$

2. $\phi\left(\prod_{i=1}^{n} a_i\right) = \prod_{i=1}^{n} \phi(a_i)$

   Realizamos inducción en n:

   - Para $n = 1$: $\phi(a_1) = \phi(a_1)$, Cierto.
   - Supuesto cierto para $n-1$, lo probamos para n:

$$\phi\left(\prod_{i=1}^{n} a_i\right) = \phi\left(\prod_{i=1}^{n-1} a_i\right)\phi(a_n) = \left(\prod_{i=1}^{n-1} \phi(a_i)\right)\phi(a_n) = \prod_{i=1}^{n} \phi(a_i)$$

3. $\phi(0) = 0$

   Por ser ϕ un homomorfismo tenemos que $\phi(0) = \phi(0+0) = \phi(0) + \phi(0)$. Por tanto:

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

4. $\phi(-a) = -\phi(a)$

$$0 = \phi(0) = \phi(a + (-a)) = \phi(a) + \phi(-a) \Longrightarrow -\phi(a) = \phi(-a)$$

5. $\phi(na) = n\phi(a)$

$$\phi(na) = \phi\left(\sum_{i=1}^{n} a\right) = \sum_{i=1}^{n} \phi(a) = n\phi(a)$$

6. $\phi(a^n) = (\phi(a))^n$ si $n \in \mathbb{N}$

$$\phi(a^n) = \phi\left(\prod_{i=1}^{n} a\right) = \prod_{i=1}^{n} \phi(a) = (\phi(a))^n$$

7. $\phi(u) \in \mathcal{U}(A') \ \wedge \ \phi(u^{-1}) = (\phi(u))^{-1}$

   Tenemos que $u \in \mathcal{U}(A)$, por lo que $\exists u^{-1} \mid u \cdot u^{-1} = 1$. Por tanto,

$$1 = \phi(1) = \phi(u \cdot u^{-1}) = \phi(u)\phi(u^{-1})$$

   Por tanto, $\phi(u) \in \mathcal{U}(A')$, con $(\phi(u))^{-1} = \phi(u^{-1})$.

8. $\phi(u^n) = (\phi(u))^n$

   Si el exponente es positivo, tenemos que se trata de un producto generalizado y, por ser un homomorfismo, se tiene de forma directa por la propiedad 2. Por tanto, vemos el caso negativo. Sea $n \in \mathbb{N}$:

$$\phi(u^{-n}) = \phi((u^{-1})^n) = (\phi(u)^{-1})^n = (\phi(u))^{-n}$$

□

Proposición 2.18. *Sean A, A' anillos conmutativos y $\phi : A \longrightarrow A'$ un homomorfismo de anillos. Entonces:*

$$Img(\phi) = \{\phi(a) \mid a \in A\} \text{ es un subanillo de } A'$$

Demostración. Es demostrar que $Img(\phi)$ es cerrado para la suma, producto y opuesto de A' y que contiene al 1 y al 0 de A'.

Sean $a', b' \in Img(\phi) \Longrightarrow \exists a, b \in A \mid \phi(a) = a' \ \wedge \ \phi(b) = b'$. Por tanto,

$$a' + b' = \phi(a) + \phi(b) = \phi(a + b) \in Img(\phi)$$
$$a'b' = \phi(a)\phi(b) = \phi(ab) \in Img(\phi)$$
$$-a' = -\phi(a) = \phi(-a) \in Img(\phi)$$

$$1 = \phi(1) \in Img(\phi) \qquad 0 = \phi(0) \in Img(\phi)$$

□

Definición 2.11. Sea $\phi : A \longrightarrow A'$ un homomorfismo de anillos, diremos que ϕ es un:

- **Epimorfismo** si ϕ es sobreyectiva (es decir, $Img(\phi) = A'$).
- **Monomorfismo** si ϕ es inyectiva.
- **Isomorfismo** si ϕ es biyectiva.

En el caso de que ϕ sea un isomorfismo, diremos que A y A' son **isomorfos**, notado $A \overset{\phi}{\cong} A'$ o simplemente. Recordamos que si $\phi : A \longrightarrow A'$ es un isomorfismo, por ser biyectiva, tenemos que

$$\exists \phi^{-1} : A' \longrightarrow A \mid \phi \circ \phi^{-1} = id_{A'} \ \wedge \ \phi^{-1} \circ \phi = id_A.$$

Proposición 2.19. *Sea $\phi : A \longrightarrow A'$ un isomorfismo, se verifica que $\phi^{-1} : A' \longrightarrow A$ es también un isomorfismo.*

Demostración. Tenemos que ϕ^{-1} es biyectiva, por lo que solo nos falta demostrar que es un homomorfismo. Sean $a', b' \in A' \Longrightarrow \phi^{-1}(a'), \phi^{-1}(b') \in A$.

Veamos en primer lugar que $\phi^{-1}(a' + b') = \phi^{-1}(a') + \phi^{-1}(b')$. Como A es cerrado para sumas, $\phi^{-1}(a') + \phi^{-1}(b') \in A$. Luego:

$$\phi(\phi^{-1}(a') + \phi^{-1}(b')) = \phi(\phi^{-1}(a')) + \phi(\phi^{-1}(b')) = a' + b' = \phi(\phi^{-1}(a' + b'))$$

Como ϕ es inyectiva, tenemos que $\phi^{-1}(a') + \phi^{-1}(b') = \phi^{-1}(a' + b')$.

Veamos ahora que $\phi^{-1}(a'b') = \phi^{-1}(a')\phi^{-1}(b')$. Como A es cerrado para productos, $\phi^{-1}(a')\phi^{-1}(b') \in A$. Luego:

$$\phi(\phi^{-1}(a')\phi^{-1}(b')) = \phi(\phi^{-1}(a'))\phi(\phi^{-1}(b')) = a'b' = \phi(\phi^{-1}(a'b'))$$

Como ϕ es inyectiva, tenemos que $\phi^{-1}(a')\phi^{-1}(b') = \phi^{-1}(a'b')$.

Veamos ahora que $\phi^{-1}(1) = 1$. Como $1 = \phi(1) \Longrightarrow \phi^{-1}(1) = \phi^{-1}(\phi(1)) = 1$. □

Ejemplo. Consideramos la proyección canónica; es decir,

$$p : \mathbb{Z} \longrightarrow \mathbb{Z}_5 \mid p(a) = [a] \qquad \forall a \in \mathbb{Z}$$

$$p(12^3) = p(12)^3 = 2^3 = 3$$

Proposición 2.20. *Sean $\phi : A \longrightarrow A'$, $\varphi : A' \longrightarrow A''$ homomorfismos de anillos, se verifica que $\varphi \circ \phi : A \longrightarrow A''$ es también un homomorfismo de anillos. Es decir, la composición de homomorfismos de anillos es un homomorfismo de anillos.*

Demostración. Sean $a, b \in A$. Veamos que cumple las tres condiciones para que sea un homomorfismo de anillos, donde para ello usamos que φ, ϕ son homomorfismos de anillos.

1. $(\varphi \circ \phi)(a+b) = (\varphi \circ \phi)(a) + (\varphi \circ \phi)(b)$.

   $(\varphi\circ\phi)(a+b) = \varphi(\phi(a+b)) = \varphi(\phi(a)+\phi(b)) = \varphi(\phi(a))+\varphi(\phi(b)) = (\varphi\circ\phi)(a)+(\varphi\circ\phi)(b)$

2. $(\varphi \circ \phi)(ab) = (\varphi \circ \phi)(a) \cdot (\varphi \circ \phi)(b)$.

   $(\varphi\circ\phi)(ab) = \varphi(\phi(ab)) = \varphi(\phi(a)\phi(b)) = \varphi(\phi(a))\varphi(\phi(b)) = (\varphi\circ\phi)(a)\cdot(\varphi\circ\phi)(b)$

3. $(\varphi \circ \phi)(1) = 1$.

   $$(\varphi \circ \phi)(1) = \varphi(\phi(1)) = \varphi(1) = 1$$

□

2.5. El anillo de los polinomios

Definición 2.12 (Copia isomorfa)**.** Sea $\iota : A \longrightarrow B$ un monomorfismo de anillos conmutativos. Entonces, $\iota : A \longrightarrow Img(\iota)$ es un isomorfismo y diremos que el anillo B contiene una **copia isomorfa** del anillo A que no es otro que su imagen por ι.

Siempre que el monomorfismo ι esté claro por el contexto no hay problema en identificar A con $Img(\iota)$. Lo que significa que si $a \in A$ y $b \in B$, escribiremos:

- ab para representar $\iota(a)b$.
- $a + b$ para representar $\iota(a) + b$.

Esto se debe a que, como no pertenecen al mismo anillo, por norma general no podemos operar entre ellos.

Ejemplo. Sea $A = \{f : [0,1] \longrightarrow \mathbb{R} \mid f \text{ aplicación}\}$.

Consideramos:

$$\begin{array}{rcl} \iota : \mathbb{R} & \longrightarrow & A \\ r & \longmapsto & \iota(r) \end{array}$$

Como $\iota(r) \in A$, tenemos que:

$$\begin{array}{rcl} \iota(r) : [0,1] & \longrightarrow & \mathbb{R} \\ t & \longmapsto & \iota(r)(t) = r \end{array}$$

Podemos ver que ι es un monomorfismo:

Probamos primero que ι es un homomorfismo. Sean $a, b \in \mathbb{R}$, $\forall t \in [0,1]$:

$$a + b = \iota(a+b)(t) = \iota(a)(t) + \iota(b)(t) = a + b$$
$$ab = \iota(ab)(t) = \iota(a)(t)\iota(b)(t) = ab$$
$$1 = \iota(1)(t)$$

A continuación, probamos que es inyectiva:

$$\forall a, b \in \mathbb{R} \mid \iota(a) = \iota(b) \Longrightarrow \forall t \in [0,1] \qquad a = \iota(a)(t) = \iota(b)(t) = b$$

Por lo visto, podemos concluir que ι define un isomorfismo $\iota : \mathbb{R} \xrightarrow{\cong} Img(\iota)$.

Es usual identificar $\mathbb{R}$ con $Img(\iota)$ y de esta forma considerar $\mathbb{R}$ como un subanillo de A. Es decir, a cada número real $r \in \mathbb{R}$ lo identificaremos con la aplicación constantemente igual a r en $[0,1]$.

Teorema 2.21. *Sea A un anillo conmutativo cualquiera. Entonces exite un anillo conmutativo P que contiene una copia isomorfa de A y un elemento que llamaremos x tal que cualquier elemento no nulo $f \in P$ se representa de forma única como:*

$$f = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n$$

Donde $f_0, f_1, f_2, \ldots, f_n \in A$ con $f_n \neq 0$ y $n \geqslant 0$.

Demostración. Definimos el anillo conmutativo S que contendrá a P como subanillo:

$$S = \{f : \mathbb{N} \longrightarrow A \mid f \text{ es aplicación}\}$$

Dado $f \in S$, escribiremos $f(n) = f_n \ \ \forall n \in \mathbb{N}$ y pondremos: $f = (f_n)_{n\geqslant 0}$ o bien $f = (f_0, f_1, \ldots, f_n, \ldots)$. Es decir, f es una sucesión de elementos de A.

Definimos la suma de $f = (f_n)_{n\geqslant 0}$y $g = (g_n)_{n\geqslant 0}$ como:

$$s = f + g = (f_n)_{n\geqslant 0} + (g_n)_{n\geqslant 0} = (f_n + g_n)_{n\geqslant 0} = (s_n)_{n\geqslant 0}$$

$$s_i = f_i + g_i \qquad \forall i \in \{0, 1, \ldots, n\}$$

Y el producto de f y g por:

$$p = f \cdot g = (p_n)_{n\geqslant 0}$$

$$p_k = \sum_{i+j=k} f_i g_j = f_n g_0 + f_{n-1} g_1 + \ldots + f_1 g_{n-1} + f_0 g_n \ \ \forall k \in \{0, \ldots, n\}$$

Comprobamos a continuación que S es un anillo conmutativo:

- La suma de S es asociativa y conmutativa gracias a la suma de A (compruébese).
- El cero de S es $0 = (0, 0, \ldots, 0, \ldots) = (0_n)_{n\geqslant 0}$, donde $0_n = 0 \ \ \forall n \in \mathbb{N}$.
- El opuesto de $f = (f_n)_{n\geqslant 0}$ es $-f := (-f_n)_{n\geqslant 0}$.

- Veamos la propiedad asociativa del producto. Sean $f = (f_n)_{n\geqslant 0}$, $g = (g_n)_{n\geqslant 0}$, $h = (h_n)_{n\geqslant 0}$:

  El término n-ésimo de $(fg)h$ es:

$$\sum_{i+j=n}\left(\sum_{u+v=i} f_u g_v\right) h_j = \sum_{u+v+j=n} f_u g_v h_j$$

  El término n-ésimo de $f(gh)$ es:

$$\sum_{i+j=n} f_i \left(\sum_{u+v=j} g_u h_v\right) = \sum_{i+u+v=n} f_i g_u h_v$$

  Como podemos ver, coinciden. Por tanto, $(fg)h = f(gh)$.

- Veamos ahora la propiedad conmutativa del producto. Sean $f = (f_n)_{n\geqslant 0}$, $g = (g_n)_{n\geqslant 0}$:

$$\left.\begin{array}{l} f\cdot g = p \mid p_k = \displaystyle\sum_{i+j=k} f_i g_j \\ g\cdot f = p \mid p_k = \displaystyle\sum_{j+i=k} g_i f_j \end{array}\right\} \Longrightarrow f\cdot g = g\cdot f$$

- Veamos la propiedad distributiva del producto. Sean $f = (f_n)_{n\geqslant 0}$, $g = (g_n)_{n\geqslant 0}$, $h = (h_n)_{n\geqslant 0}$:

$$\left.\begin{array}{l} f(g+h) = p \mid p_k = \displaystyle\sum_{i+j=k} f_i(g_j + h_j) \\ fg + fh = p \mid p_k = \displaystyle\sum_{i+j=k} f_i g_j + \sum_{i+j=k} f_i h_j = \sum_{i+j=k} f_i(g_j+h_j) \end{array}\right\} \Longrightarrow f(g+h) = fg+fh$$

- El uno del anillo es la sucesión $1 = (1, 0, 0, \ldots, 0)$:

$$(1\cdot f)_k = f_k\cdot 1 + f_{k-1}\cdot 0 + \ldots + f_1\cdot 0 + f_0\cdot 0 = f_k \quad k\in\{0,\ldots,n\} \Longrightarrow 1\cdot f = f$$

Por tanto, tenemos que S es un anillo conmutativo.

Definimos ahora la aplicación $\iota : A \longrightarrow S$ por:

$$\iota(a) = (a, 0, 0, \ldots, 0, \ldots) \qquad \forall a\in A$$

Veamos en primer lugar que ι es un homomorfismo de anillos. Sean $a, b \in A$:

1. $\iota(a+b) = (a+b, 0, 0, \ldots, 0, \ldots) = (a, 0, 0, \ldots, 0, \ldots) + (b, 0, 0, \ldots, 0, \ldots) = \\ = \iota(a) + \iota(b)$.

2. $\iota(ab) = (ab, 0, 0, \ldots, 0, \ldots) \overset{(*)}{=} (a, 0, 0, \ldots, 0, \ldots)(b, 0, 0, \ldots, 0, \ldots) = \iota(a)\iota(b)$

   Donde en $(*)$ hemos aplicado que:

- Si $n \geqslant 1$, $\iota(ab)_n = \sum_{i+j=n} \iota(a)_i \iota(b)_j$. Si $i+j=n$, como $n \geqslant 1$, tenemos que:

$$\left\{ \begin{array}{ccc} i \geqslant 1 & \Longrightarrow & \iota(a)_i = 0 \\ \vee & & \vee \\ j \geqslant 1 & \Longrightarrow & \iota(b)_j = 0 \end{array} \right\}$$

- Si $n = 0$, $\iota(ab)_0 = \sum_{i+j=0} \iota(a)_i \iota(b)_j = \iota(a)_0 \iota(b)_0 = ab$.

3. $\iota(1) = (1, 0, 0, \ldots, 0, \ldots) = 1$.

Por tanto, tenemos que ι es un homomorfismo de anillos. Veamos que, en concreto, es un monomorfismo. Supuestos $a, b \in A \mid \iota(a) = \iota(b)$. Entonces:

$$(a, 0, \ldots, 0, \ldots) = \iota(a) = \iota(b) = (b, 0, \ldots, 0, \ldots) \Longrightarrow a = b \Longrightarrow \iota \text{ inyectiva}$$

$\iota : A \longrightarrow S$ es un monomorfismo por lo que S contiene a A como copia isomorfa. Identificaremos A con $Img(\iota)$ en S. Esto es, a implicará $(a, 0, \ldots, 0, \ldots) \in S \ \ \forall a \in A$.

Denotaremos por x al elemento de S definido por:

$$x = (0, 1, 0, \ldots, 0, \ldots)$$

Es decir, x es la sucesión cuyos términos son 0 excepto el término $n = 1$ que es $1 \in A$. Tenemos por tanto, que $\forall a \in A$:

$$ax = (a, 0, \ldots, 0, \ldots)(0, 1, 0, \ldots, 0, \ldots)$$

Veamos el resultado de dicho producto:

$$(ax)_n = \sum_{i+j=n} a_i x_j = a_n x_0 + a_{n-1} x_1 + \ldots + a_1 x_{n-1} + a_0 x_n 0$$

- Para $n = 0$:

$$(ax)_0 = \sum_{i+j=0} a_i x_j = a_0 x_0 = a \cdot 0 = 0$$

- Para $n = 1$:

$$(ax)_1 = \sum_{i+j=1} a_i x_j = a_1 x_0 + a_0 x_1 = 0 \cdot 0 + a \cdot 1 = a$$

- Para $n > 1$:

$$(ax)_{n>1} = \sum_{i+j=n} a_i x_j = a_n x_0 + a_{n-1} x_1 + \ldots + a_1 x_{n-1} + a_0 x_n = 0 + 0 \cdot 1 + \ldots + 0 + 0 = 0$$

Por tanto, tenemos que:

$$ax = (0, a, 0, \ldots, 0, \ldots)$$

Veamos el efecto de multiplicar x por $f = (f_n)_{n \geqslant 0} \in S$:

$$xf = (0, 1, 0, \ldots, 0, \ldots)(f_0, f_1, \ldots, f_k, \ldots)$$

- Para $n = 0$:
$$(xf)_0 = x_0 f_0 = 0 \cdot f_0 = 0$$
- Para $n = 1$:
$$(xf)_1 = x_1 f_0 + x_0 f_1 = 1 \cdot f_0 + 0 \cdot f_1 = f_0$$
- Para $n = 2$:
$$(xf)_2 = x_2 f_0 + x_1 f_1 + x_0 f_2 = 0 + 1 \cdot f_1 + 0 = f_1$$
- Para $n = k \in \{1, 2, \dots\}$:
$$(xf)_k = x_k f_0 + x_{k-1} f_1 + \ldots + x_1 f_{k-1} + x_0 f_k = 0 + 0 + \ldots + f_{k-1} + 0 = f_{k-1}$$

Por tanto, tenemos que:

$$xf = (0, f_0, f_1, \dots, f_{k-1}, \dots)$$

De lo anterior, se deduce que

$$\forall k \geqslant 1 \qquad x^k = (0, 0, \dots, \underbrace{1}_{k}, \dots, 0, \dots)$$
$$\forall a \in A \qquad ax^k = (0, 0, \dots, \underbrace{a}_{k}, \dots, 0, \dots)$$

Definimos P como el subconjunto de S formado por aquellas sucesiones que tienen todos sus términos 0 salvo un número finito. Es decir, $f \in P$ si $\exists n \in \mathbb{N}$ tal que $f_k = 0 \ \ \forall k \geqslant n + 1$. Por tanto, $f \in P$ es de la forma:

$$f = (f_0, f_1, \dots, f_n, 0, 0, \dots, 0, \dots)$$

Veamos que P es un subanillo de S. Sean $n, m \in \mathbb{N}$ y $f = (f_0, f_1, \dots, f_n, 0, \dots)$, $g = (g_0, g_1, \dots, g_m, 0, \dots) \ \in P$:

1. P es cerrado para sumas:
$$f + g = (f_0, \dots, f_n, 0, \dots) + (g_0, \dots, g_m, 0, \dots)$$
   - Si $n = m$:
   $$f + g = (f_0 + g_0, f_1 + g_1, \dots, f_n + g_n, 0, \dots) \in P$$
   - Si $n > m$:
   $$f + g = (f_0 + g_0, f_1 + g_1, \dots, f_m + g_m, f_{m+1}, \dots, f_n, 0, \dots) \in P$$
   - Si $m > n$:
   $$f + g = (f_0 + g_0, f_1 + g_1, \dots, f_n + g_n, g_{n+1}, \dots, g_m, 0, \dots) \in P$$

   Por lo que P es cerrado para la suma de S.

2. P es cerrado para el producto:
   Para ello, observemos que $(fg)_k = 0 \qquad \forall k > n+m$:

$$(fg)_k = \sum_{i+j=k} f_i g_j$$

   Si $k = i+j > n+m \Longrightarrow \left\{ \begin{array}{ccc} i > n & \Longrightarrow & f_i = 0 \\ \vee & & \vee \\ j > m & \Longrightarrow & g_j = 0 \end{array} \right\} \Longrightarrow f_i g_j = 0$. Por tanto, se tiene que $fg \in P$, por lo que es cerrado para el producto.

3. P es cerrado para opuestos:

$$-f = (-f_0, -f_1, \ldots, -f_n, 0, \ldots, 0, \ldots) \in P$$

4. $0, 1 \in P$:

$$0 = (0, 0, \ldots, 0, \ldots) \in P \qquad 1 = (1, 0, 0, \ldots, 0, \ldots) \in P$$

Por lo que P es un subanillo de S.

Tenemos además que P contiene una copia isomorfa de A ya que anteriormente identificamos cualquier $a \in A$ como $(a, 0, 0, \ldots, 0, \ldots) \in P$ y tenemos además que $x = (0, 1, 0, \ldots, 0, \ldots) \in P$.

Por tanto, tenemos ya demostrada la existencia del anillo P anunciado en el teorema. Falta ver que cualquier elemento $f \in P$ no nulo puede expresarse de forma única como:

$$f = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n$$

Para ello, aplicamos los resultados ya demostrados en este teorema:

$$\begin{aligned} f &= f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n = \\ &= (f_0, 0, \ldots, 0, \ldots) + (0, f_1, 0, \ldots, 0, \ldots) + \ldots + (0, \ldots, \underbrace{f_n}_{n}, 0, \ldots) = \\ &= (f_0, f_1, f_2, \ldots, f_n, 0, \ldots, 0, \ldots) \end{aligned}$$

Como dos elementos de P son iguales si y sólo si sus términos son iguales término a término, tenemos que podemos expresar de forma única cualquier elemento f no nulo de P de la forma buscada. □

Definición 2.13 (Anillo de polinomios)**.** El anillo P del teorema anterior se llama **anillo de polinomios en la indeterminada x con coeficientes en el anillo conmutativo** A, denotado por $A[x]$. A sus elementos los llamaremos polinomios.

Respecto a los polinomios, tenemos que:

- Si $f \in A[x] \mid f \neq 0, \quad f = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n$ lo escribiremos también como:

$$f = \sum_{i=0}^{n} f_i x^i$$

- Si $f \in A[x] \mid f \neq 0$ y sus términos son todos 0 a partir del término n-ésimo, diremos que f **es de grado** n y lo notaremos $grd(f) = n$. Por convenio, al polinomio 0 se le asigna el grado $-\infty$.
- Cada $f_i x^i$ recibe el nombre de **monomio** o término de f.
- Al término $f_n x^n$ se le llama **término líder** y a f_n le llamamos **coeficiente líder**.
- Al término f_0 se le llama **término independiente**.
- Si $f_n = 1$, diremos que f es un polinomio **mónico**.
- Los polinomios de grado 0 (los de la forma $f = a, \quad a \neq 0$), junto con el polinomio 0 se les llama **polinomios constantes**.

Notación. A veces, dado $f = \sum_{i=0}^{n} f_i x^i \in A[x]$, utilizaremos la notación $f(x)$ para referirnos al polinomio f. Es decir:

$$f = f(x) = \sum_{i=0}^{n} f_i x^i$$

En el anillo de polinomios, tenemos que para $f = \sum_{i=0}^{n} f_i x^i$, $g = \sum_{j=0}^{m} g_j x^j \ \in A[x]$ con $n > m$, la suma y el producto vienen dados por:

$$f + g = \sum_{i=0}^{n} f_i x^i + \sum_{j=0}^{m} g_j x^j = \sum_{j=0}^{m} (f_j + g_j) x^j + \sum_{i=m}^{n} f_i x^i$$

$$fg = \left(\sum_{i=0}^{n} f_i x^i \right) \left(\sum_{j=0}^{m} g_j x^j \right) = \sum_{i,j} f_i x^i g_j x^j = \sum_{i,j} f_i g_j x^{i+j} = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} f_i g_j \right) x^k$$

Ejemplo. Sea $A = \mathbb{Z}_4$, $f = 1 + 3x + 3x^7$, $g = 3 + 2x \in \mathbb{Z}_4[X]$:

$$f + g = 0 + x + 3x^7 = x + 3x^7$$
$$fg = 2 + 3x + 2x^2 + x^7 + 2x^8$$

Proposición 2.22. *Sean $f, g \in A[x]$. Entonces:*

$$grd(f + g) \leqslant \text{máx}\{grd(f), grd(g)\}$$
$$grd(fg) \leqslant grd(f) + grd(g)$$

Demostración. Sean $f, g \in A[x] \mid grd(f) = n, \ grd(g) = m$; es decir, $f = \sum_{i=0}^{n} f_i x^i$ y $g = \sum_{j=0}^{m} g_j x^j$. Sabemos que: $\begin{cases} i > n \Longrightarrow f_i = 0 \\ j > m \Longrightarrow g_j = 0 \end{cases}$. Por tanto:

$$f + g = \sum_{i=0}^{\text{máx}\{m,n\}} (f_i + g_i) \Longrightarrow grd(f + g) \leqslant \text{máx}\{n, m\}$$

$$fg = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} f_i g_j \right) x^k \Longrightarrow grd(fg) \leqslant n + m$$

□

También podemos afirmar que en $\mathbb{Z}$ se da la igualdad en el caso del producto, pero para ello hemos de introducir antes el concepto de Dominio de Integridad, que corresponde al siguiente tema.

Ejemplo.

1. Sean $f = 2 + 3x + x^2$, $g = 1 - x - x^2 \in \mathbb{Z}[x]$:

$$f + g = 3 + 2x \Longrightarrow grd(f+g) < \text{máx}\{grd(f), grd(g)\}$$
$$fg = 2 + x - 4x^2 - 4x^3 - x^4 \Longrightarrow grd(fg) = grd(f) + grd(g)$$

2. Sean $f = 1 + 2x$, $g = 2x \in \mathbb{Z}_4[x]$:

$$fg = 2x \Longrightarrow grd(fg) < grd(f) + grd(g)$$

Vemos que, en este caso, no se da la igualdad en el producto.

Teorema 2.23 (Propiedad universal del anillo de polinomios)**.** *Sean A, B anillos conmutativos y $\phi : A \longrightarrow B$ un homomorfismo de anillos conmutativos. Entonces, $\forall b \in B \;\; \exists_1 \phi_b : A[x] \longrightarrow B$ tal que:*

1. $\phi_b(a) = \phi(a), \quad \forall a \in A,$
2. $\phi_b(x) = b.$

Demostración. Demostramos primero la existencia del homomorfismo:

Definimos $\phi_b : A[x] \longrightarrow B$ para cada $f(x) = \sum_{i=0}^{n} a_i x^i \neq 0$ como:

$$\phi_b(0) = 0 \qquad \phi_b(f) = \sum_{i=0}^{n} \phi(a_i) b^i$$

Para demostrar el resultado, consideramos los siguientes polinomios:

$$f(x) = \sum_{i=0}^{n} a_i x^i, \;\; g(x) = \sum_{i=0}^{m} c_i x^i \in A[x]$$

Comprobemos en primer lugar que se trata de un homomorfismo:

1. $\phi_b(f+g) = \phi_b(f) + \phi_b(g)$

$$\phi_b(f+g) = \phi_b\left(\sum_{i=0}^{\text{máx}\{m,n\}} (f_i + g_i)x^i\right) = \sum_{i=0}^{\text{máx}\{m,n\}} \phi(f_i + g_i) b^i =$$
$$= \sum_{i=0}^{\text{máx}\{m,n\}} \left((\phi(f_i) + \phi(g_i))b^i\right) = \sum_{i=0}^{\text{máx}\{m,n\}} \left(\phi(f_i)b^i + \phi(g_i)b^i\right) =$$
$$= \sum_{i=0}^{n} \phi(f_i) b^i + \sum_{i=0}^{m} \phi(g_i) b^i = \phi_b(f) + \phi_b(g)$$

2. $\phi_b(fg) = \phi_b(f)\phi_b(g)$

$$\phi_b(fg) = \phi_b\left(\sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_i b_j\right)\right) = \sum_{k=0}^{n+m}\phi\left(\sum_{i+j=k} a_i b_j\right) b^k =$$
$$= \sum_{k=0}^{n+m}\left(\sum_{i+j=k}\phi(a_i)\phi(b_j)\right) b^k = \left(\sum_{i=0}^{n}\phi(a_i)b^i\right)\left(\sum_{j=0}^{m}\phi(b_j)b^j\right) =$$
$$= \phi_b(f)\phi_b(g)$$

3. $\phi_b(1) = 1$

$$\phi_b(1) = \sum_{i=0}^{0}\phi(1)b^i = \phi(1)b^0 = \phi(1) = 1$$

Falta ver que cumple las dos condiciones pedidas para este homomorfismo en concreto:

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

$$\forall a \in A \;\; \phi_b(a) = \sum_{i=0}^{0}\phi(a)b^i = \phi(a)b^0 = \phi(a)$$

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

$$\phi_b(x) = \sum_{i=0}^{1}\phi(x_i)b^i = x_0b^0 + x_1b^1 = 0 + b = b$$

Comprobemos ahora la unicidad del homomorfismo. Suponemos que $\exists\psi : A[x] \longrightarrow B$ homomorfismo tal que:

$$\psi(a) = \phi(a), \;\; \forall a \in A \qquad\qquad \psi(x) = b$$

Sea $f = \sum_{i=0}^{n} a_i x^i \in A[x]$. Entonces, $\forall f \in A[X]$, se tiene que:

$$\psi(f) = \psi\left(\sum_{i=0}^{n} a_i x^i\right) \overset{(*)}{=} \sum_{i=0}^{n}\psi(a_i x^i) \overset{(*)}{=} \sum_{i=0}^{n}\psi(a_i)\psi(x)^i = \sum_{i=0}^{n}\phi(a_i)b^i = \phi_b(f)$$

donde, en $(*)$, hemos empleado que ψ es un homomorfismo. Por tanto, se tiene que $\psi = \phi$. □

Definición 2.14 (Homomorfismo de evaluación de polinomios)**.** Sea $A \subset B$ un subanillo de un anillo conmutativo B. Podemos considerar el homomorfismo inclusión de A en B. Es decir, el homomorfismo

$$\begin{array}{rcl} i : A & \longrightarrow & B \\ a & \longmapsto & a \end{array}$$

Entonces, por el teorema anterior tomando $\phi = i$, se tiene que $\forall b \in B, \;\; \exists_1$ homomorfismo $ev_b : A[x] \longrightarrow B$ tal que:

1. $ev_b(a) = a, \quad \forall a \in A$,

2. $ev_b(x) = b$.

Llamaremos a este homomorfismo **homomorfismo de evaluación** en el elemento $b \in B$. Este cumple que:

$$\forall f(x) = \sum_{i=0}^{n} a_i x^i \in A[x], \qquad ev_b(f) = \sum_{i=0}^{n} a_i b^i$$

Será usual notar $ev_b(f)$ por $f(b)$.

Para realizar $f(b)$ será tan fácil como sustituir el elemento x por b y operar dentro del anillo B. Es importante notar que evaluar es un homomorfismo, luego son triviales las propiedades:

$$(f+g)(b) = f(b) + g(b) \qquad (fg) = f(b)g(b) \qquad \forall b \in B$$

Ejemplo.

1. Consideramos $A = \mathbb{Z}$, $B = \mathbb{Q}$, y sea el polinomio $f = 2 + x^2 \in \mathbb{Z}[x]$:

$$f\left(\frac{1}{2}\right) = 2 + \left(\frac{1}{2}\right)^2 = 2 + \frac{1}{4} = \frac{9}{4}$$

2. Consideramos $A = B = \mathbb{Z}$, y sea el polinomio $g = 1 + 2x + x^2 \in \mathbb{Z}[x]$:

$$g(-1) = 1 - 2 + 1 = 0$$

3. Consideramos $A = \mathbb{Z}$, $B = \mathbb{C}$, y sea el polinomio $h = (x^2+1)^2 + (x-1)^2 \in \mathbb{Z}[i]$:

$$h(i) = (i^2+1)^2 + (i-1)^2 = i^2 - 2i + 1 = -2i$$

   Notemos que no desarrollamos el producto para obtener un polinomio porque evaluar es un polinomio.

Definición 2.15 (Raíz de un polinomio)**.** Sea A un subanillo de un anillo conmutativo B, sea $f \in A[x]$. Un elemento $b \in B$ decimos que es una **raíz** o un cero del polinomio f si $f(b) = 0$.

Teorema 2.24 (Homomorfismo inducido en el anillo de polinomios)**.** *Sea $\phi : A \longrightarrow B$ un homomorfismo cualquiera de anillos conmutativos. Entonces, existe un único homomorfismo $\phi : A[x] \longrightarrow B[x]$ (el cual no debe confundirse con el homomorfismo $\phi : A \longrightarrow B$) tal que:*

1. $a \longmapsto \phi(a) \qquad \forall a \in A$

2. $x \longmapsto x$

Este está definido por:

$$\phi\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \phi(a_i) x^i$$

Llamaremos a este homomorfismo $\phi : A[x] \longrightarrow B[x]$ *el* ***homomorfismo inducido en los anillos de polinomios****.*

Demostración. Este resultado es un corolario directo de la Propiedad Universal del Anillo de Polinomios aplicado al homomorfismo $i \circ \phi$, donde i es la inclusión. Veámoslo:

$$A \xrightarrow{\phi} B \xrightarrow{i} B[x] \qquad i \circ \phi : A \longrightarrow B[x]$$

Como la composición de homomorfismos es un homomorfismo, tenemos que $i \circ \phi$ es un homomorfismo de anillos. Entonces, considerando $b = x \in B[x]$, la Propiedad Universal del Anillo de Polinomios aplicada a $i \circ \phi$ nos afirma que existe un único homomorfismo tal que:

1. $(i \circ \phi)_x(a) \overset{(*)}{=} (i \circ \phi)(a) = i(\phi(a)) = \phi(a)$
2. $(i \circ \phi)_x(x) \overset{(*)}{=} x$

donde en $(*)$ he aplicado la Propiedad Universal del Anillo de Polinomios.

Además, también afirma que dicho homomorfismo se define $\forall f = \sum_{i=0}^{n} a_i x^i$ por:

$$(i \circ \phi)_x(0) = 0 \qquad (i \circ \phi)_x(f) = \sum_{i=0}^{n} (i \circ \phi)(a_i) x^i = \sum_{i=0}^{n} \phi(a_i) x^i$$

por lo que demuestra directamente el resultado enunciado. □

Ejemplo.

1. Consideramos el homomorfismo $R_2 : \mathbb{Z} \longrightarrow \mathbb{Z}_2 \mid R_2(a) = R(a; 2) \ \ \forall a \in \mathbb{Z}$.

   $R_2 : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_2[x]$ es el homomorfismo inducido en los anillos de polinomios. Por ser un homomorfismo:

   $$R_2(5 + 8x^2 + 3x^6) = 1 + x^6$$
   $$R_2((7x^2 + 3)(5x + 1) + 7) = R_2(7x^2 + 3) R_2(5x + 1) + R_2(7) =$$
   $$= (x^2 + 1)(x + 1) + 1 = x^3 + x^2 + x$$

2. Para $n \geqslant 2$, tenemos $R_n : \mathbb{Z} \longrightarrow \mathbb{Z}_n \mid R_n(a) = R(a; n) \qquad \forall a \in \mathbb{Z}$.

   $R_n : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_n[x]$ es el homomorfismo inducido por R_n en los anillos de polinomios.

   $$R_n\left(\sum_{i=0}^{k} a_i x^i\right) = \sum_{i=0}^{k} R_n(a_i) x^i = \sum_{i=0}^{k} R(a; n) x^i$$

3. Divisibilidad en Dominios Euclídeos

Consideramos la ecuación: $ax = b$ con $a, b \in A$, $a \neq 0$.

- Si A es un cuerpo, la ecuación tiene solución única: $x = a^{-1}b$.
- Si A no es un cuerpo, no tenemos asegurada la existencia de la solución en A:

$$2x = 3 \quad \text{no tiene solución en } \mathbb{Z}$$

Puede ocurrir además que la ecuación tenga más de una solución en A:

$$2x = 2 \qquad \left\{ \begin{array}{c} x = 1 \\ \wedge \\ x = 4 \end{array} \right\} \text{ en } \mathbb{Z}_6$$

Definición 3.1 (Dominio de Integridad)**.** Un **dominio de integridad** (abreviado a partir de ahora como DI) es un anillo conmutativo A no trivial en el que se verifica la propiedad cancelativa, que dice:

$$\left. \begin{array}{c} ab = ac \\ a \neq 0 \end{array} \right\} \Longrightarrow b = c \qquad \forall a, b, c \in A$$

Lema 3.1. *En un DI, la ecuación $ax = b$, con $a \neq 0$, si tiene solución necesariamente es única.*

Demostración. Supongamos que $\exists x, x' \in A \mid ax = b \ \wedge \ ax' = b$.

$$b = b \Longrightarrow ax = ax' \text{ con } a \neq 0 \Longrightarrow x = x'$$

□

Proposición 3.2 (Caracterización de un DI)**.** *Sea A un anillo conmutativo no trivial. Entonces:*

$$A \text{ es DI} \iff \forall a, b \in A \mid a, b \neq 0 \text{ se tiene que } ab \neq 0$$

Equivalente, su contrarrecíproco es:

$$A \text{ es DI} \iff \forall a, b \in A \mid ab = 0 \text{ se tiene que } a = 0 \ \vee \ b = 0$$

Demostración.

$\Longrightarrow$) Sea A un DI y sean $a, b \in A \mid ab = 0$. Supongamos $a \neq 0$ sin perder generalidad y sabemos que $a \cdot 0 = 0$ luego:

$$\left.\begin{array}{c} ab = 0 = a \cdot 0 \\ a \neq 0 \end{array}\right\} \overset{A \text{ es DI}}{\Longrightarrow} b = 0$$

$\Longleftarrow$) Supongamos que en A se verifica la propiedad enunciada. Entonces, $\forall a, b, c \in A$ con $a \neq 0$ y $ab = ac$, se tiene que:

$$ab = ac \Longrightarrow ab - ac = a(b - c) = 0$$

Por la propiedad enunciada, como $a \neq 0$ se tiene que $b - c = 0$, por lo que $b = c$ y se tiene que es un DI.

□

Lema 3.3. *Si K es un cuerpo $\Longrightarrow$ K es un dominio de integridad.*

Demostración. K es un cuerpo $\Longrightarrow$ K es un anillo conmutativo no trivial.

Para todo $a, b, c \in k$ con $a \neq 0$ y $ab = ac$, se tiene que:

$$ab = ac \Longrightarrow a^{-1}(ab) = a^{-1}(ac) \Longrightarrow b = c$$

donde he aplicado que, como $a \neq 0$, es una unidad. Por tanto, se tiene que es un DI. □

Como corolario tenemos que $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}[\sqrt{n}] \mid (n \in \mathbb{Z} \ \ \sqrt{n} \notin \mathbb{Z})$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, etc. son dominios de integridad.

Lema 3.4. *Si B es DI y A es subanillo de $B \Longrightarrow A$ es DI.*

Demostración. Por reducción al absurdo. Como A no es DI, tenemos que $\exists a, b, c \in A \mid a \neq 0$ tal que $ab = ac$ pero $b \neq c$. No obstante, como $A \subset B$, tenemos que lo escrito también se aplica a B y por tanto B no es un DI, por lo que llegamos a una contradicción. □

Por tanto, $\mathbb{Z}$, $\mathbb{Z}[\sqrt{n}] \mid (n \in \mathbb{Z} \ \ \sqrt{n} \notin \mathbb{Z})$, etc. son dominios de integridad.

Ejemplo. Algunos ejemplos de anillos conmutativos que no son dominios de integridad son: $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_8$:

$$\begin{aligned} 2 \in \mathbb{Z}_4 \mid 2 \neq 0 \text{ pero } 2 \cdot 2 = 0 &\Longrightarrow \mathbb{Z}_4 \text{ no es DI} \\ 2, 3 \in \mathbb{Z}_6 \mid 2, 3 \neq 0 \text{ pero } 2 \cdot 3 = 0 &\Longrightarrow \mathbb{Z}_6 \text{ no es DI} \\ 2, 4 \in \mathbb{Z}_8 \mid 2, 4 \neq 0 \text{ pero } 2 \cdot 4 = 0 &\Longrightarrow \mathbb{Z}_8 \text{ no es DI} \end{aligned}$$

Teorema 3.5. *Sea A un anillo conmutativo no trivial. Entonces:*

$$A \text{ es DI} \Longleftrightarrow A[x] \text{ es DI}$$

Demostración.

$\Longrightarrow$) Si $A[x]$ es DI, como A es subanillo de $A[x] \Longrightarrow A$ es DI.

$\Longleftarrow$) Supongamos que A es DI. Sean $f, g \in A[x] \mid f, g \neq 0$:

$$f = \sum_{i=0}^{n} a_i x^i \quad g = \sum_{j=0}^{m} b_j x^j \mid grd(f) = n \ \wedge \ grd(g) = m \Longrightarrow a_n, b_m \neq 0$$

Por el producto de polinomios, tenemos que:

$$fg = \sum_{k=0}^{n+m} d_k x^k \mid d_k = \sum_{i+j=k} a_i b_j$$

Sabemos que si $\left\{ \begin{array}{ccc} i > n & \Longrightarrow & a_i = 0 \\ & \wedge & \\ j > m & \Longrightarrow & b_j = 0 \end{array} \right\}$. En particular:

$$d_{n+m} = \sum_{i+j=n+m} a_i b_j = a_n b_m \neq 0$$

por ser A un DI y $a_n, b_m \neq 0$. Deducimos entonces que $fg \neq 0$, por lo que $A[x]$ es DI.

□

Lema 3.6. *Sea A un DI y $f, g \in A[x] \mid f, g \neq 0$. Entonces:*

$$grd(fg) = grd(f) + grd(g)$$

Demostración. Suponemos que:

$$f = \sum_{i=0}^{n} a_i x^i \quad g = \sum_{j=0}^{m} b_j x^j \mid grd(f) = n \ \wedge \ grd(g) = m \Longrightarrow a_n, b_m \neq 0$$

Por el producto de polinomios, se tiene que:

$$fg = \sum_{k=0}^{n+m} d_k x^k \mid d_k = \sum_{i+j=k} a_i b_j$$

Tenemos que $d_{n+m} = \sum_{i+j=n+m} a_i b_j = a_n b_m \neq 0$, como hemos demostrado en el lema anterior. Se tiene por tanto que $grd(fg) = n + m = grd(f) + grd(g)$. □

Proposición 3.7. *Sea A un DI. Entonces:*

$$\mathcal{U}(A) = \mathcal{U}(A[x])$$

Demostración. Como A es subanillo de $A[x]$, es claro que $\mathcal{U}(A) \subseteq \mathcal{U}(A[x])$. Veamos la otra inclusión.

Consideramos $f \in \mathcal{U}(A[x]) \Longrightarrow \exists g \in \mathcal{U}(A[x]) \mid fg = 1$.

$$grd(f) + grd(g) = grd(fg) = grd(1) = 0 \Longrightarrow grd(f) = 0 \ \wedge \ grd(g) = 0$$

Por tanto, $f \in A \ \wedge \ g \in A \mid fg = 1 \Longrightarrow f, g \in \mathcal{U}(A) \Longrightarrow \mathcal{U}(A[x]) \subseteq \mathcal{U}(A)$.

Tenemos entonces que $\mathcal{U}(A) = \mathcal{U}(A[x])$ por la doble inclusión. □

Proposición 3.8. *Sea A un anillo conmutativo finito no trivial:*

$$A \text{ es DI} \iff A \text{ es un cuerpo}$$

Demostración.

$\Longrightarrow$) Vista en el Lema 3.3.

$\Longleftarrow$) Supongamos que A es DI y cogemos $a \in A \mid a \neq 0$. Consideramos la aplicación $\lambda : A \to A \mid \lambda(x) = ax \ \ \forall x \in A$.

Es claro que λ es inyectiva: $\forall b, c \in A \mid \lambda(b) = \lambda(c) \Longrightarrow ab = ac \overset{A \text{ DI}}{\Longrightarrow} b = c$. Como A es finito, por la Proposición 1.20 se tiene que λ es sobreyectiva, por lo que $Img(\lambda) = A$.

Como $1 \in A = Img(\lambda)$, se tiene que $\exists b \in A \mid \lambda(b) = ab = 1$. Por tanto, tenemos que $a \in \mathcal{U}(A) \ \ \forall a \in A \setminus \{0\}$; es decir, A es un cuerpo.

□

3.1. Cuerpo de fracciones de un dominio de integridad

Sea A un DI, consideramos $A \times (A \setminus \{0\}) = \{(a, s) \mid a, s \in A, \ s \neq 0\}$.
Definimos la relación binaria notada $\sim$ definida por:

$$(a, s) \sim (b, t) \iff at = bs \qquad \forall (a, s), (b, t) \in A \times (A \setminus \{0\})$$

Notemos que $\sim$ es una relación de equivalencia:

1. Reflexividad:

$$\forall (a, s) \in A \times (A \setminus \{0\}) \qquad as = as \Longrightarrow (a, s) \sim (a, s)$$

2. Simetría:

$$\forall (a, s), (b, t) \in A \times (A \setminus \{0\}) \mid (a, s) \sim (b, t) \Longrightarrow at = bs \Longrightarrow bs = at \Longrightarrow (b, t) \sim (a, s)$$

3. Transitividad: $\forall (a, s), (b, t), (c, u) \in A \times (A \setminus \{0\}) \mid (a, s) \sim (b, t) \sim (c, u)$

$$\left.\begin{array}{l}(a, s) \sim (b, t) \Longrightarrow at = bs \\ (b, t) \sim (c, u) \Longrightarrow bu = ct\end{array}\right\} \Longrightarrow atu = bsu = bus = cts \Longrightarrow tau = tcs \overset{\text{DI}}{\underset{t \neq 0}{\Longrightarrow}}$$
$$\Longrightarrow au = cs \Longrightarrow (a, s) \sim (c, u)$$

Consideramos el conjunto cociente $A \times (A \setminus \{0\}) / \sim$, que denotaremos $\mathbb{Q}(A)$. Para todo $(a, s) \in A \times (A \setminus \{0\})$, su clase de equivalencia la notaremos $\dfrac{a}{s} =: [(a, s)]$ y leeremos la fracción de numerador a y denominador s.

$$\mathbb{Q}(A) = \left\{ \frac{a}{s} \mid a, s \in A \ \wedge \ s \neq 0 \right\}$$

Notemos que $\frac{a}{s} = \frac{b}{t} \iff (a,s) \sim (b,t) \iff at = bs, \qquad \forall a,b,s,t \in A \mid s,t \neq 0.$

Definimos en $\mathbb{Q}(A)$ una suma y un producto a partir de la suma y el producto de A como:

$$\frac{a}{s} + \frac{b}{t} := \frac{at+bs}{st} \qquad \frac{a}{s}\frac{b}{t} := \frac{ab}{st} \qquad \forall\ \frac{a}{s}, \frac{b}{t} \in \mathbb{Q}(A)$$

Tenemos que ver que la suma y el producto están bien definidos, es decir, que no dependen del representante de la clase:

$$\forall\ \frac{a_1}{s_1} = \frac{a_2}{s_2},\ \frac{b_1}{t_1} = \frac{b_2}{t_2} \in \mathbb{Q}(A) \Longrightarrow a_1 s_2 = a_2 s_1\ \wedge\ b_1 t_2 = b_2 t_1$$

Comprobamos en primer lugar que la suma está bien definida:

$$\frac{a_1}{s_1} + \frac{b_1}{t_1} = \frac{a_1 t_1 + b_1 s_1}{s_1 t_1} \qquad \frac{a_2}{s_2} + \frac{b_2}{t_2} = \frac{a_2 t_2 + b_2 s_2}{s_2 t_2}$$

Veamos si son iguales ambas fracciones:

$$\begin{aligned}(a_1 t_1 + b_1 s_1) s_2 t_2 &= a_1 t_1 s_2 t_2 + b_1 s_1 s_2 t_2 = a_1 s_2 t_1 t_2 + b_1 t_2 s_1 s_2 = \\ &= a_2 s_1 t_1 t_2 + b_2 t_1 s_1 s_2 = a_2 t_2 s_1 t_1 + b_2 s_2 s_1 t_1 = (a_2 t_2 + b_2 s_2) s_1 t_1\end{aligned}$$

Luego ambas fracciones son iguales y, por tanto, la suma está bien definida. Veamos ahora el producto:

$$\frac{a_1}{s_1}\frac{b_1}{t_1} = \frac{a_1 b_1}{s_1 t_1} \qquad \frac{a_2}{s_2}\frac{b_2}{t_2} = \frac{a_2 b_2}{s_2 t_2}$$

Veamos si ambas fracciones son iguales:

$$(a_1 b_1)(s_2 t_2) = (a_1 s_2)(b_1 t_2) = (a_2 s_1)(b_2 t_1) = (a_2 b_2) s_1 t_1$$

Por tanto, también tenemos que el producto está bien definido.

Lema 3.9. $\mathbb{Q}(A)$ *es un anillo conmutativo con la suma y el producto especificados.*

Demostración. Para todo $\frac{a}{s}, \frac{b}{t}, \frac{c}{u} \in \mathbb{Q}(A)$, veamos que se cumplen las condiciones necesarias:

1. Asociativa de la suma:

$$\left(\frac{a}{s} + \frac{b}{t}\right) + \frac{c}{u} = \frac{at+bs}{st} + \frac{c}{u} = \frac{u(at+bs)+cst}{stu} = \frac{uat+ubs+cst}{stu}$$

$$\frac{a}{s} + \left(\frac{b}{t} + \frac{c}{u}\right) = \frac{a}{s} + \frac{bu+ct}{tu} = \frac{atu+s(bu+ct)}{stu} = \frac{uat+ubs+cst}{stu}$$

2. Conmutativa de la suma:

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} = \frac{bs+at}{ts} = \frac{b}{t} + \frac{a}{s}$$

3. Neutro de la suma: $\frac{0}{1} \in \mathbb{Q}(A)$.

$$\frac{0}{1} + \frac{a}{s} = \frac{a \cdot 1 + s \cdot 0}{s \cdot 1} = \frac{a}{s}$$

4. Existencia de opuesto:

$$\frac{-a}{s} \in \mathbb{Q}(A) \mid \frac{a}{s} + \frac{-a}{s} = \frac{as + (-a)s}{s^2} = \frac{s(a-a)}{s^2} = \frac{a-a}{s} = \frac{0}{s} = \frac{0}{1}$$

5. Asociativa del producto:

$$\left(\frac{a}{s}\frac{b}{t}\right)\frac{c}{u} = \frac{ab}{st}\frac{c}{u} = \frac{abc}{stu} \qquad \frac{a}{s}\left(\frac{b}{t}\frac{c}{u}\right) = \frac{a}{s}\frac{bc}{tu} = \frac{abc}{stu}$$

6. Conmutativa del producto:

$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st} = \frac{ba}{ts} = \frac{b}{t}\frac{a}{s}$$

7. Neutro del producto: $\frac{1}{1} \in \mathbb{Q}(A)$.

$$\frac{a}{s}\frac{1}{1} = \frac{a \cdot 1}{s \cdot 1} = \frac{a}{s}$$

8. Propiedad distributiva:

$$\frac{a}{s}\left(\frac{b}{t} + \frac{c}{u}\right) = \frac{a}{s}\frac{bu + ct}{tu} = \frac{a(bu+ct)}{stu} = \frac{abu + act}{stu}$$

$$\frac{a}{s}\frac{b}{t} + \frac{a}{s}\frac{c}{u} = \frac{ab}{st} + \frac{ac}{su} = \frac{absu + stac}{stsu} = \frac{s(abu+act)}{sstu} = \frac{abu+act}{stu}$$

□

Lema 3.10. $\mathbb{Q}(A)$ *es un cuerpo.*

Demostración. Tenemos que es un anillo, por lo que para ver que es un cuerpo solo falta por demostrar que todos sus elementos no nulos son unidades. Entonces, $\forall\ \frac{a}{s} \in \mathbb{Q}(A) \mid \frac{a}{s} \neq \frac{0}{1}$, consideramos $\frac{s}{a}$. Veamos que $\left(\frac{a}{s}\right)^{-1} = \frac{s}{a}$:

$$\frac{a}{s}\frac{s}{a} = \frac{as}{sa} = \frac{1}{1} \Longrightarrow \frac{a}{s} \in \mathcal{U}(\mathbb{Q}(A)) \ \ \forall\ \frac{a}{s} \in A \setminus \left\{\frac{0}{1}\right\}$$

□

Llamamos a $\mathbb{Q}(A)$ el **cuerpo de fracciones del anillo** A. Notemos que $\mathbb{Q}(\mathbb{Z}) = \mathbb{Q}$.

Lema 3.11. $\mathbb{Q}(A)$ *contiene una copia isomorfa de* A.

Demostración. Definimos $j : A \to \mathbb{Q}(A) \mid j(a) = \frac{a}{1} \ \ \forall a \in A$. Veamos que j es un homomorfismo. $\forall a, b \in A$:

$$j(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = j(a) + j(b)$$
$$j(ab) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1} = j(a)j(b)$$
$$j(1) = \frac{1}{1}$$

Veamos ahora que j es un monomorfismo. $\forall a, b \in A \mid j(a) = j(b)$:

$$\frac{a}{1} = j(a) = j(b) = \frac{b}{1} \iff a = b$$

Hemos podido definir un monomorfismo $j : A \to \mathbb{Q}(A)$ luego $\mathbb{Q}(A)$ contiene una copia isomorfa de A y nos será usual identificar A con $Img(j)$. Vemos así A como subanillo de $\mathbb{Q}(A)$. □

Lema 3.12. *Si K es un cuerpo. Entonces $\mathbb{Q}(K) = K$.*

Demostración. Es claro que $K \subseteq \mathbb{Q}(K)$ por el Lema 3.11. Veamos ahora la otra inclusión. Para todo $\frac{a}{s} \in \mathbb{Q}(K)$, por definición del cuerpo de fracciones se tiene que $a, s \in K$, $s \neq 0$. Además, como K es un cuerpo, consideramos s^{-1}. Por tanto:

$$\frac{a}{s} = \frac{as^{-1}}{ss^{-1}} = \frac{as^{-1}}{1} \in K$$

Luego $\mathbb{Q}(K) \subseteq K$ y por doble inclusión tenemos que $\mathbb{Q}(K) = K$. □

Por tanto, podemos utilizar en cualquier cuerpo K la notación de fracciones:

$$\frac{a}{s} =: as^{-1} \qquad s \neq 0$$

Ejemplo. En $\mathbb{Z}_5$, se tiene que:

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

Lema 3.13. *Si A y B son DI con A subanillo de B. Entonces $\mathbb{Q}(A)$ es subanillo de $\mathbb{Q}(B)$.*

Demostración. Para todo $\frac{a}{s} \in \mathbb{Q}(A)$, se tiene que:

$$a, s \in A \ \wedge \ s \neq 0 \Longrightarrow a, s \in B \ \wedge \ s \neq 0 \Longrightarrow \frac{a}{s} \in \mathbb{Q}(B)$$

□

Lema 3.14. *Si A es DI y subanillo de un cuerpo K, entonces $\mathbb{Q}(A)$ es subcuerpo (subanillo y cuerpo) de K.*

Es decir, $\mathbb{Q}(A)$ es el menor cuerpo que contiene a A.

Demostración. $\mathbb{Q}(A)$ es subanillo de $\mathbb{Q}(K) = K$ por ser A subanillo de K y sabemos que $\mathbb{Q}(A)$ es un cuerpo. □

3.2. Divisibilidad en un dominio de integridad

Definición 3.2 (Divisor)**.** Sea A un DI y sean $a, b \in A$. Diremos que a **divide a** b o que a **es un divisor de** b si:

$$\exists c \in A \mid b = ca.$$

En tal caso, escribiremos $a|b$. Diremos también que b es un **múltiplo** de a.

Es decir: $\forall a, b \in A$:

$$a|b \iff \exists c \in A \mid b = ca$$

Notemos que decir que $a|b$ es decir que, si $a \neq 0$, entonces la ecuación $ax = b$ tiene solución única en A:

$$ax = b \ \wedge \ a|b, \ a \neq 0 \Longrightarrow \exists c \in A \mid b = ca \Longrightarrow ax = ca \Longrightarrow x = c$$

Notemos además que $0|b \iff b = 0$:

$$0|b \iff \exists c \in A \mid b = c \cdot 0 \iff b = 0$$

Notación. Dado $a \in A$ con A DI, notaremos por $Div(a)$ al conjunto de todos los divisores de a:

$$Div(a) = \{b \in A \mid b|a\}$$

Notación. Sea A un DI, y sea $a, b \in A$. En el caso de que a no divida a b, lo notaremos mediante $a \nmid b$.

Lema 3.15. *Sea A un DI con $a, b \in A$, $a \neq 0$:*

$$a|b \iff \frac{b}{a} \in A$$

Demostración.

$\Longrightarrow$) Se tiene que, por definición, $a|b \iff \exists c \in A \mid b = ca$. Por tanto,

$$\frac{b}{a} = \frac{ca}{a} = \frac{c}{1} \in A$$

$\Longleftarrow$) Suponiendo que $\dfrac{b}{a} \in A$, se tiene que:

$$\frac{b}{a} \in A \Longrightarrow \exists c \in A \mid \frac{b}{a} = \frac{c}{1} \Longrightarrow b = ca \Longrightarrow a|b$$

□

Proposición 3.16. *Algunas propiedades que cumple la divisibilidad son, para todo $a, b, c \in A \mid a, b, c \neq 0$,*

1. *Reflexividad. $a|a \qquad \forall a \in A$,*
2. *Transitividad. Si $a|b \ \wedge \ b|c \Longrightarrow a|c$,*

3. Si $a|b \ \wedge \ a|c \Longrightarrow a|bx+cy \qquad \forall x,y \in A,$

4. $a|b \Longleftrightarrow ac|bc.$

Demostración.

1. Reflexividad. $a|a \qquad \forall a \in A,$

$$\forall a \in A \mid a \neq 0 \Longrightarrow \exists\ 1 \in A \mid a = a \cdot 1 \Longrightarrow a|a$$

2. Transitividad. Si $a|b \ \wedge \ b|c \Longrightarrow a|c,$

$$a|b \Longrightarrow \exists d \in A \mid b = da$$
$$b|c \Longrightarrow \exists e \in A \mid c = eb$$

Probamos por tanto el resultado buscado:

$$c = eb = eda \Longrightarrow \exists ed \in A \mid c = eda \Longrightarrow a|c.$$

3. Si $a|b \ \wedge \ a|c \Longrightarrow a|bx+cy \qquad \forall x,y \in A,$
Como $a|b \ \wedge \ a|c$, tenemos que:

$$a|b \Longrightarrow \exists d \in A \mid b = da$$
$$a|c \Longrightarrow \exists e \in A \mid c = ea$$

Por tanto, tenemos que:

$$bx + cy = dax + eay = (dx + ey)a \Longrightarrow a|bx + cy$$

4. $a|b \Longleftrightarrow ac|bc.$

$\Longrightarrow$) Como $a|b$, tenemos que $\exists d \in A \mid b = da$. Por tanto,

$$bc = dac \Longrightarrow ac|bc$$

$\Longleftarrow$) Partimos desde que $ac|bc$, por lo que:

$$ac|bc \Longrightarrow \exists d \in A \mid bc = dac \Longleftrightarrow bc - dac = 0 \Longleftrightarrow c(b - da) = 0 \Longleftrightarrow$$
$$\Longleftrightarrow b - da = 0 \Longleftrightarrow b = da \Longrightarrow a|b$$

□

Estaremos interesados en conocer los divisores de cualquier elemento $b \in A$ siendo A un DI. En el caso de que sea $b = 0$, es trivial ya que todos los elementos del anillo son sus divisores:

$$a|0 \Longleftrightarrow \exists c \in A \mid 0 = ac \Longrightarrow a|0 \ \ \forall a \in A \text{ siendo } c = 0.$$

Es decir, $Div(0) = A$. Estudiemos por tanto los cosos en los que $b \neq 0$.

Lema 3.17. *Sea* A *un DI con* $b \in A \mid b \neq 0$. *Si* $u \in \mathcal{U}(A)$. *Entonces* $u|b$.

Demostración. Partiendo de que $u|b \iff \exists c \in A \mid b = uc$, tenemos que

$$b = u(u^{-1}b) \implies u|b$$

por lo que es cierto, tomando $c = u^{-1}b$. □

Así pues, $\mathcal{U}(A)$ es un conjunto de divisores de b. Es decir, $\mathcal{U}(A) \subset Div(b)$.

Lema 3.18. *Sea A un DI. Si $u \in \mathcal{U}(A)$:*

$$a|u \iff a \in \mathcal{U}(A)$$

Es decir: $Div(u) = \mathcal{U}(A)$.

Demostración.

$\impliedby$) Por el lema anterior, tenemos que $a|u$.

$\implies$) $a|u \implies \exists c \in A \mid u = ca \implies 1 = u^{-1}ca \implies a \in \mathcal{U}(A)$.

□

Definición 3.3 (Asociados)**.** Sea A un DI y $a, b \in A \mid a, b \neq 0$. Diremos que a y b **son asociados**, notado $a \sim b$ si:

$$a|b \ \wedge \ b|a$$

Lema 3.19. *La relación binaria de ser asociados, $\sim$, es una relación de equivalencia.*

Demostración. Demostramos las tres condiciones:

1. Reflexividad: $\forall a \in A \mid a \neq 0 \implies \exists\ 1 \in A \mid a = a \cdot 1 \implies a|a \implies a \sim a$.
2. Simetría: $\forall a, b \in A \mid a, b \neq 0 \ \wedge \ a \sim b \implies a|b \ \wedge \ b|a \implies b|a \ \wedge \ a|b \implies b \sim a$.
3. Transitividad: $\forall a, b, c \in A \mid a, b, c \neq 0$, tenemos que:

$$\left\{ \begin{array}{ccc} a \sim b & \implies & a|b \ \wedge \ b|a \\ & \wedge & \\ b \sim c & \implies & b|c \ \wedge \ c|a \end{array} \right\} \implies \left\{ \begin{array}{ccc} a|b \wedge b|c & \implies & a|c \\ & \wedge & \\ c|b \wedge b|a & \implies & c|a \end{array} \right\} \implies a \sim c.$$

□

Proposición 3.20 (Caracterización de los asociados)**.** *Sea A un DI con $a, b \in A \mid a, b$ no nulos. Entonces:*

$$a \sim b \iff \exists u \in \mathcal{U}(A) \mid a = ub$$

(De donde se deduce que que $b = u^{-1}a$).

Demostración.

$\implies$) Sea $a \sim b \implies a|b \ \wedge \ b|a \implies \exists u, v \in A \mid b = ua \ \wedge \ a = vb$. Entonces:

$$b = ua = uvb \implies b(1 - uv) = 0 \underset{b \neq 0}{\overset{\text{DI}}{\implies}} (1 - uv) = 0 \implies uv = 1 \implies u, v \in \mathcal{U}(A)$$

$\Longleftarrow$) Suponemos que $\exists u \in \mathcal{U}(A) \mid a = ub$ Entonces, por ser $u \in \mathcal{U}(A)$, tenemos que $b = u^{-1}a$. Por tanto,

$$\left.\begin{array}{rcl} a = ub & \Longrightarrow & b|a \\ & \wedge & \\ b = u^{-1}a & \Longrightarrow & a|b \end{array}\right\} \Longrightarrow a \sim b.$$

□

Lema 3.21. *Sea A un DI, y sean $a, b \in A \mid a, b \neq 0$ tal que $a \sim b$. Entonces, $\forall c \in A$ se cumple que:*

$$c|a \Longleftrightarrow c|b$$

Es decir, $a \sim b \Longrightarrow Div(a) = Div(b)$.

Demostración.

$\Longrightarrow$) $c|a \ \wedge \ a \sim b \Longrightarrow c|a \ \wedge \ a|b \Longrightarrow c|b.$

$\Longleftarrow$) $c|b \ \wedge \ a \sim b \Longrightarrow c|b \ \wedge \ b|a \Longrightarrow c|a.$

□

Por definición, el conjunto de todos los asociados a b, son siempre divisores de b. Es decir,

$$\{a \in A \mid a \sim b\} = \{ub \in A \mid u \in \mathcal{U}(A)\} \subset Div(b).$$

Definición 3.4 (Divisores triviales)**.** Sea A un DI, dado $b \in A$, diremos que los **divisores triviales** de b son las unidades y sus asociados. Es decir, el conjunto de los divisores triviales de b es el conjunto:

$$\mathcal{U}(A) \cup \{ub \mid u \in \mathcal{U}(A)\} \subset Div(b)$$

Ejemplo. Veamos algunos ejemplos de divisores triviales:

1. En $\mathbb{Z}$, sabemos que $\mathcal{U}(\mathbb{Z}) = \{\pm 1\}$. Entonces, dado $b \in \mathbb{Z}$, sus divisores triviales son: $\{-1, 1, -b, b\}$.

2. En $\mathbb{Z}[i]$, sabemos que $\mathcal{U}(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. Entonces, dado $\alpha \in \mathbb{Z}[i]$, sus divisores triviales son: $\{\pm 1, \pm i, \pm\alpha, b - ai, -b + ai\}$.

Definición 3.5 (Irreducible)**.** Sea A un DI. Un elemento $a \in A$ diremos que es **irreducible** si $a \neq 0$, $a \notin \mathcal{U}(A)$ y sus únicos divisores son los triviales:

$$Div(a) = \mathcal{U}(A) \cup \{ua \mid u \in \mathcal{U}(A)\}$$

Ejemplo. En $\mathbb{Z}$, tenemos que:

- El 2 es irreducible: $Div(2) = \{-1, 1, -2, 2\}$.
- El 4 no lo es: $Div(4) = \{-1, 1, -4, 4\}$.

Proposición 3.22 (Caracterización de irreducibles)**.** *Sea A un DI, $a \in A$ tal que $a \neq 0 \ \wedge \ a \notin \mathcal{U}(A)$. Entonces:*

$$a \text{ es irreducible } \iff \forall b, c \in A \mid a = bc \text{ se tiene que } \begin{cases} b \in \mathcal{U}(A) \\ \vee \\ c \in \mathcal{U}(A) \end{cases}$$

Demostración.

$\Longrightarrow$) Demostramos mediante reducción al absurdo.

Sea $a = bc$ con $b, c \in A$. Supongamos que $b, c \notin \mathcal{U}(A)$. Como $a = bc$, tenemos que $b|a \ \wedge \ c|a$ y, por ser a irreducible, se tiene que b, c son divisores triviales de a.

Como $b, c \notin \mathcal{U}(A) \Longrightarrow b \sim a \ \wedge \ c \sim a \Longrightarrow \exists u, v \in \mathcal{U}(A) \mid b = ua \ \wedge \ c = va$. Por tanto,

$$a = bc = ua \cdot va = a^2uv \Longrightarrow 1 = auv \Longrightarrow a \in \mathcal{U}(A) \text{ Contradicción.}$$

Luego $b \in \mathcal{U}(A) \ \vee \ c \in \mathcal{U}(A)$.

$\Longleftarrow$) Sea b un divisor de a, es decir, $\exists c \in A \mid a = bc$. Entonces:

- Si $b \in \mathcal{U}(A) \Longrightarrow b$ es divisor trivial de a.
- Si $c \in \mathcal{U}(A) \Longrightarrow b = c^{-1}a \Longrightarrow b \sim a \Longrightarrow b$ es divisor trivial de a.

Por lo que a es irreducible ya que todos sus divisores son triviales.

□

3.3. Dominios Euclídeos

Definición 3.6 (Dominio Euclídeo)**.** Un **Dominio Euclídeo** (abreviado DE) es un DI A junto con una aplicación

$$\phi : A \setminus \{0\} \to \mathbb{N}$$

Llamada **función euclídea** de A tal que:

1. $\phi(ab) \geqslant \phi(a) \qquad \forall a, b \in A \mid a, b \neq 0,$
2. $\forall a, b \in A \mid b \neq 0 \qquad \exists q, r \in A \mid a = bq + r, \text{ con } \begin{cases} r = 0 \\ \vee \\ \phi(r) < \phi(b) \end{cases}$

A dichos q y r los llamaremos cociente y resto de dividir a entre b, respectivamente.

Observación. Notemos que en la definición de DE no se exige la unicidad de q y r.

Proposición 3.23. *$\mathbb{Z}$ es un DE con función euclídea $|\cdot| : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ la función valor absoluto.*

Demostración. Sabemos que $\mathbb{Z}$ es un DI, visto como consecuencia del Lema 3.4.

Veamos que el valor absoluto verifica la primera condición:

$$\forall a, b \in \mathbb{Z} \mid a, b \neq 0 \Longrightarrow |ab| = |a||b| \geqslant |a| \qquad (b \neq 0 \Longrightarrow |b| \geqslant 1)$$

Sabemos que se verifica la segunda condición gracias al Teorema 2.5. □

Proposición 3.24. *Sea A DE y $a, b \in A \mid a, b \neq 0$, 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) $\Longrightarrow$ 2) $b|a \Longrightarrow \exists c \in A \mid a = bc$. Supogamos que $q, r \in A$ son cociente y resto de dividir a entre b. Entonces, por la definición de DE, tenemos que

$$a = qb + r \qquad r = 0 \ \vee \ \phi(r) < \phi(b)$$

Supongamos que $r \neq 0 \Longrightarrow \phi(r) < \phi(b)$.

$$a = bq + r \Longrightarrow r = a - bq = bc - bq = b(c - q)$$

$$\phi(r) = \phi(b(c - q)) \overset{(1)}{\geqslant} \phi(b) \text{ Contradicción.}$$

Luego $r = 0$.

2) $\Longrightarrow$ 3) Trivial, ya que 2) es una generalización de 3).

3) $\Longrightarrow$ 1) Al ser 0 un resto de dividir a entre b, tenemos que $\exists q \in A \mid a = bq \Longrightarrow b|a$.

□

Teorema 3.25. *Sea K un cuerpo y $f, g \in K[x] \mid g \neq 0$.*

Entonces, existen únicos $q, r \in K[x] \mid f = gq + r$ con $\begin{cases} r = 0 \\ \vee \\ grd(r) < grd(g) \end{cases}$

Demostración. Supuesta la existencia, comenzamos demostrando su unicidad:

Sea $\begin{cases} f = gq + r & \text{con} \quad r = 0 \quad \vee \quad grd(r) < grd(g) \\ f = gq' + r' & \text{con} \quad r' = 0 \quad \vee \quad grd(r') < grd(g') \end{cases}$

- Si $r = r' \Longrightarrow gq + r = gq' + r' \Longrightarrow gq = gq' \Longrightarrow q = q'$.
- Si $r \neq r'$, tenemos que alguno de los dos no es nulo. Por tanto, tenemos que $grd(r') < grd(g) \vee grd(r) < grd(g)$. Independientemente, tenemos que $r - r' \neq 0 \ \wedge \ grd(r - r') < grd(g)$. Entonces:

$$gq + r = gq' + r' \Longrightarrow r - r' = g(q' - q) \Longrightarrow grd(r - r') = grd(g(q' - q)) = \\ = grd(g) + grd(q' - q) \geqslant grd(g) \quad \text{Contradicción.}$$

donde he aplicado que el grado del producto es la suma de los grados, ya que A es un DI por ser un cuerpo. Por tanto, estamos en el caso anterior.

Procedemos ahora a demostrar la existencia del cociente y del resto. Sean $f, g \in K[x] \mid g \neq 0$:

- Si $f = 0 \Longrightarrow q = 0 \ \wedge \ r = 0$.
- Si $f \neq 0 \ \wedge \ grd(f) < grd(g) \Longrightarrow q = 0 \ \wedge \ r = f$.
- Si $f \neq 0 \ \wedge \ grd(f) = n \geqslant m = grd(g)$:

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + \ldots + a_1 x + a_0 \quad \text{con } a_n \neq 0$$
$$g(x) = \sum_{j=0}^{m} b_j x^j = a_m x^m + \ldots + b_1 x + b_0 \quad \text{con } b_m \neq 0$$

Hacemos inducción en $n = grd(f)$:

- Si $n = 0$: $f = a_0 \neq 0$ y como $n \geqslant m \Longrightarrow m = 0$ y $g = b_0 \neq 0$. Como K es un cuerpo, $\exists b_0^{-1} \in K$. Luego:

$$q = b_0^{-1} a_0 \ \wedge \ r = 0 \Longrightarrow gq + r = b_0 b_0^{-1} a_0 = a_0 = f$$

- Supuesto cierto para $n-1$, lo probamos para $n > 0$:
  Consideramos el siguiente polinomio:

$$\begin{aligned} f_1 &= f - b_m^{-1} a_n x^{n-m} g(x) = \\ &= a_n x^n + \ldots + a_1 x + a_0 - b_m^{-1} a_n x^{n-m}(b_m x^m + \ldots + b_1 x + b_0) = \\ &= f - \underbrace{a_n x^n} + b_m^{-1} a_n b_{m-1} x^{n-1} + \ldots + b_m^{-1} a_n b_1 x^{n-m+1} + b_m^{-1} a_n b_0 x^{n-m} \end{aligned}$$

  Tenemos que el término n-ésimo de f se cancela con el destacado y por tanto $grd(f_1) \ \leqslant \ n-1$. Por hipótesis de inducción, tenemos que:

$$\exists q_1, r_1 \in K[x] \mid f_1 = gq_1 + r_1 \text{ con } r_1 = 0 \ \vee \ grd(r_1) < grd(g)$$

  Por tanto, como $f_1 = f - b_m^{-1} a_n x^{n-m} g = gq_1 + r_1$ se tiene que:

$$f = gq_1 + r_1 + b_m^{-1} a_n x^{n-m} g = g(\underbrace{b_m^{-1} a_n x^{n-m} + q_1}_{q}) + r_1$$

  Por tanto, tenemos que el cociente y el resto buscados son:

$$q = b_m^{-1} a_n x^{n-m} + q_1 \qquad r = r_1$$

Por tanto, queda demostrada la existencia también. □

Corolario 3.25.1. *Si K es un cuerpo. Entonces $K[x]$ es un DE con función euclídea:*

$$grd : K[x] \setminus \{0\} \to \mathbb{N}$$

Demostración. Como K es un cuerpo, tenemos que $K[x]$ es un DI. Veamos que efectivamente el grado es una función euclídea:

1. $\forall f, g \in K[x] \mid f, g \neq 0 \Longrightarrow grd(fg) = grd(f) + grd(g) \geqslant grd(f)$.
2. Existen únicos $q, r \in K[x] \mid f = gq + r$ con $r = 0 \ \vee \ grd(r) < grd(g)$, como vimos en el teorema anterior.

□

Ejemplo. Veamos algunos ejemplos de divisiones de polinomios:

1. En $\mathbb{Q}[x]$, comprobar si el polinomio $g = 2x^4 - 3x^2 + 6x + 10$ es un divisor del polinomio $f = 6x^6 - 9x^5 + 2x^4 + 15x^3 + 30x^2 + 8x + 10$.

$$\begin{array}{rrrrrr|l}
6x^6 - 9x^5 & +2x^4 + 15x^3 + 30x^2 & & +8x + 10 & & 2x^4 - 3x^2 + 6x + 10 \\
\cline{6-6}
-6x^6 & +9x^4 - 18x^3 - 30x^2 & & & & 3x^2 - \frac{9}{2}x + \frac{11}{2} \\
\cline{1-4}
 & -9x^5 + 11x^4 & -3x^3 & +8x & & \\
 & 9x^5 & -\frac{27}{2}x^3 + 27x^2 + 45x & & & \\
\cline{2-4}
 & & 11x^4 - \frac{33}{2}x^3 + 27x^2 + 53x + 10 & & & \\
 & -11x^4 & +\frac{33}{2}x^2 - 33x - 55 & & & \\
\cline{2-4}
 & & -\frac{33}{2}x^3 + \frac{87}{2}x^2 + 20x - 45 & & &
\end{array}$$

   Por tanto, como $r \neq 0 \Longrightarrow g \not| f$.

   Notemos que $3x^2 = \frac{1}{2} \cdot 6 \cdot c^{6-4} = b_m^{-1} a_n x^{n-m}$ es el factor que aparece en la demostración del teorema anterior.

2. En $\mathbb{Z}_5[x]$, comprobar si $g = 3x^2 + 1$ es divisor de $f = 2x^4 + 4x^3 + 3x + 2$.

$$\begin{array}{rrrrr|l}
2x^4 & +4x^3 & & +3x & +2 & 3x^2 + 1 \\
\cline{5-5}
-2x^4 & & -4x^2 & & & 4x^2 + 3x + 2 \\
\cline{1-3}
 & 4x^3 & +x^2 & +3x & & \\
 & -4x^3 & & -3x & & \\
\cline{2-4}
 & & x^2 & & +2 & \\
 & & -x^2 & & -2 & \\
\cline{3-5}
 & & & & 0 &
\end{array}$$

   Por tanto, tenemos que $r = 0$ y que $g|f$.

Teorema 3.26. *Para $n = -2, -1, 2, 3$, el anillo $\mathbb{Z}[\sqrt{n}]$ es un DE con función euclídea:*

$$\phi : \mathbb{Z}[\sqrt{n}] \setminus \{0\} \to \mathbb{N} \qquad \phi(\alpha) = |N(\alpha)| \ \ \forall \alpha \in \mathbb{Z}[\sqrt{n}]$$

Demostración. Para que sea un DE, su función euclídea ha de cumplir dos condiciones:

1. $\phi(\alpha\beta) \geqslant \phi(\alpha), \qquad \forall \alpha, \beta \in \mathbb{Z}[\sqrt{n}] \setminus \{0\}$.

$$\phi(\alpha\beta) = |N(\alpha\beta)| = |N(\alpha)N(\beta)| = |N(\alpha)||N(\beta)| \geqslant |N(\alpha)| = \phi(\alpha)$$

2. $\exists q, r \in \mathbb{Z}[\sqrt{n}] \mid \alpha = q\beta + r$, con $r = 0 \ \vee \ \phi(r) < \phi(\beta)$. Realizamos la siguiente distinción de casos:

   - Si $\phi(\alpha) = |N(\alpha)| < |N(\beta)| = \phi(\beta) \Longrightarrow q = 0 \ \wedge \ r = \alpha$.
   - Si $\phi(\alpha) \geqslant \phi(\beta)$:
     Sean $\alpha = a + b\sqrt{n}, \beta = c + d\sqrt{n} \neq 0$. Como $\beta \neq 0$, entonces $N(\beta) \neq 0$. Por tanto, en $\mathbb{Q}[\sqrt{n}]$ consideramos el sguiente elemento:

$$\alpha \cdot \beta^{-1} = \frac{\alpha}{\beta} = \frac{\alpha \cdot \overline{\beta}}{\beta \cdot \overline{\beta}} = \frac{(a + b\sqrt{n})(c - d\sqrt{n})}{N(\beta)} = \\ = \frac{(ac - nbd) + (cb - ad)\sqrt{n}}{N(\beta)} = \frac{ac - nbd}{N(\beta)} + \frac{cb - ad}{N(\beta)}\sqrt{n}$$

     Sea $a_1 := \dfrac{ac - nbd}{N(\beta)}$ y $a_2 := \dfrac{cb - ad}{N(\beta)}$; es decir, $\dfrac{\alpha}{\beta} = a_1 + a_2\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$.
     Elegimos $q_1, q_2 \in \mathbb{Z} \mid |a_1 - q_1| \leqslant \dfrac{1}{2}$ y $|a_2 - q_2| \leqslant \dfrac{1}{2}$. Sea $q = q_1 + q_2\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ y $r := \alpha - q\beta \in \mathbb{Z}[\sqrt{n}]$.
     Se tiene entonces que hemos encontrado $q, r \in \mathbb{Z}[\sqrt{n}] \mid \alpha = q\beta + r$. Falta ver que $r = 0 \ \vee \ \phi(r) < \phi(\beta)$.

     Supongamos que $r \neq 0$, y trabajamos en $\mathbb{Q}[\sqrt{n}]$:

$$\phi(r) = |N(r)| = |N(\alpha - q\beta)| = \left|N\left(\beta\left(\frac{\alpha}{\beta} - q\right)\right)\right| = \left|N(\beta)N\left(\frac{\alpha}{\beta} - q\right)\right| = \\ = |N(\beta)| \cdot \left|N\left(\frac{\alpha}{\beta} - q\right)\right| = |N(\beta)| \cdot |N[(a_1 - q_1) + (a_2 - q_2)\sqrt{n}]| = \\ = |N(\beta)| \cdot |(a_1 - q_1)^2 - n(a_2 - q_2)^2|$$

     Sea $A = (a_1 - q_1)^2 - n(a_2 - q_2)^2$, y realizamos la distinción de casos siguiente:

     - Si $n = -2$:

$$A = (a_1 - q_1)^2 + 2(a_2 - q_2)^2 \leqslant \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{4}\right)^2 = \frac{3}{4} \Longrightarrow |A| < 1$$

     - Si $n = -1$:

$$A = (a_1 - q_1)^2 + (a_2 - q_2)^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} \Longrightarrow |A| < 1$$

     - Si $n = 2$:

$$A = (a_1 - q_1)^2 - 2(a_2 - q_2)^2 \leqslant \left(\frac{1}{2}\right)^2 - \frac{1}{2} \Longrightarrow \frac{-1}{2} \leqslant A \leqslant \frac{1}{4} \Longrightarrow |A| < 1$$

     - Si $n = 3$:

$$A = (a_1 - q_1)^2 - 3(a_2 - q_2)^2 \leqslant \left(\frac{1}{2}\right)^2 - 3\left(\frac{1}{2}\right)^2 \Longrightarrow \frac{-3}{4} \leqslant A \leqslant \frac{1}{4} \Longrightarrow |A| < 1$$

Por tanto, en dichos casos tenemos que $|A| < 1$. Por tanto,

$$\phi(r) = |N(\beta)||A| \leqslant |N(\beta)| = \phi(\beta)$$

□

Ejemplo. Dividir $\alpha = 11 + 7i$ entre $\beta = 2i$ en $\mathbb{Z}[i]$.

Buscamos $q, r \in \mathbb{Z}[i] \mid \alpha = q\beta + r$ con $r = 0 \ \vee \ \phi(r) < \phi(\beta)$. Consideramos en $\mathbb{Q}[i]$ el siguiente elemento:

$$\frac{\alpha}{\beta} = \frac{11+7i}{2i} = \frac{(11+7i)(-2i)}{4} = \frac{14-22i}{4} = \frac{7}{2} - \frac{11}{2}i$$

Elegimos $q_1, q_2 \in \mathbb{Z} \mid \left|\frac{7}{2} - q_1\right| \leqslant \frac{1}{2} \ \wedge \ \left|\frac{11}{2} - q_2\right| \leqslant \frac{1}{2}$.

1. Tomamos, por ejemplo $q_1 = 3 \ \wedge \ q_2 = -5 \Longrightarrow q = 3 - 5i$.

$$r = \alpha - q\beta = (11 - 7i) - 2i(3 - 5i) = 1 + i$$
$$11 + 7i = q\beta + r \ \wedge \ \phi(r) = N(1+i) = 2 < 4 = N(2i) = \phi(\beta)$$

2. Podemos elegir también $q_1' = 4 \ \wedge \ q_2' = -6 \Longrightarrow q' = 4 - 6i$.

$$r' = \alpha - q'\beta = (11 - 7i) - 2i(4 - 6i) = -1 - i$$
$$11 + 7i = q'\beta + r' \ \wedge \ \phi(r) = N(-1-i) = 2 < 4 = N(2i) = \phi(\beta)$$

Por tanto, acabamos de ver que el cociente y el resto en $\mathbb{Z}[i]$ no son únicos.

3.4. Máximo Común Divisor

Definición 3.7 (Máximo común divisor)**.** Sea A un DI y $a, b \in A$. Un **máximo común divisor** de a y b, notado $\text{mcd}(a, b)$ es $d \in A$ tal que:

1. $d|a \ \wedge \ d|b$,
2. Si $c \in A \mid c|a \ \wedge \ c|b \Longrightarrow c|d$.

De la definición se tiene por tanto que:

$$Div(d) = Div(a) \cap Div(b)$$

Observación. No siempre existe el máximo común divisor de dos elementos.

Además, si existe no es único. Para verlo, sea $d = \text{mcd}(a, b)$, y consideramos $du \mid u \in \mathcal{U}(A)$. Entonces:

1. Como $du|d$, y se tiene que $d|a \wedge d|b$, por transitividad se tiene que $du|a \wedge du|b$.
2. Análogamente, si $c \in A$ cumple que $c|d$ por ser este el $\text{mcd}(a, b)$, la transitividad afirma que $c|du$ al tener que $d|du$.

Por tanto, hemos visto que $du = \text{mcd}(a, b)$. De forma general, tenemos que el mcd de dos elementos, si existe, es único salvo asociados. Hablaremos simplemente del mcd de a y b.

Definición 3.8 (Máximo común divisor generalizado)**.** Sea A un DI y consideramos $a_1, a_2, \ldots, a_n \in A (n \geqslant 2)$. Un máximo común divisor de $a_1, a_2, \ldots, a_n$, notado como $\text{mcd}(a_1, a_2, \ldots, a_n)$ es $d \in A$ tal que verifica:

1. $d|a_i \ \ \forall i \in \{1, \ldots, n\}$,
2. Si $c \in A \mid c|a_i \ \ \forall i \in \{1, \ldots, n\} \Longrightarrow c|d$.

Definición 3.9 (Primos relativos)**.** Sean $a, b \in A$. Diremos que a y b son **primos relativos** si $\text{mcd}(a, b) = 1$.

Propiedades del mcd**.** Sea A DI, supuesta la existencia de los mcd que intervienen, tenemos que:

1. $\text{mcd}(a, b) = \text{mcd}(b, a)$. En general:

   $$\text{mcd}(a_1, \ldots, a_i, a_{i+1}, \ldots, a_n) = \text{mcd}(a_1, \ldots, a_{i+1}, a_i, \ldots, a_n) \ \ n \geqslant 2, \ i \in \{1, \ldots, n-1\}$$

   La demostración es trivial, ya que en la definición no se establece ningún orden.

2. Si $a \sim a'$, entonces $\text{mcd}(a, b) = \text{mcd}(a', b)$.

   Sea $d = \text{mcd}(a, b)$. Entonces, $d|a$. Además, por ser $a \sim a'$, se tiene que $a|a'$. Por la transitividad, $d|a'$. Además, se tiene también que $d|b$, por lo que la primera condición se tiene.

   Veamos la segunda. Como $a \sim a'$, tenemos que $c|a \Longleftrightarrow c|a'$, por lo que $\forall c \in A$ se tiene que si $c|a' \wedge c|b$, entonces $c|a \wedge c|b$; y por tanto $c|d$. Por tanto, se deduce que $d = \text{mcd}(a', b)$.

3. $\text{mcd}(a, b) = a \Longleftrightarrow a|b$. Particularmente, $\text{mcd}(a, 0) = a \ \wedge \ \text{mcd}(a, 1) = 1$.

   $\Longrightarrow$) $\text{mcd}(a, b) = a \Longrightarrow a|a \ \wedge \ a|b$.

   $\Longleftarrow$) Partimos de que $a|b$. Además, por la reflexividad se tiene que $a|a$. Entonces, se tiene la primera condición para que sea $a = \text{mcd}(a, b)$.

   Además, como $\forall c \in A \mid c|a \ \wedge \ c|b$ se tiene que $c|a$, tenemos también la segunda condición, por lo que $a = \text{mcd}(a, b)$.

4. $\text{mcd}(\text{mcd}(a, b), c) = \text{mcd}(a, b, c) = \text{mcd}(a, \text{mcd}(b, c))$.

   Demostramos en primer lugar la primera igualdad. Sea $d = \text{mcd}(\text{mcd}(a, b), c)$. Por tanto, $d|\,\text{mcd}(a, b) \wedge d|c$. Además, como $\text{mcd}(a, b)|a$ y $\text{mcd}(a, b)|b$, por la transitividad se tiene que $d|a \wedge d|b$, por lo que se tiene la primera condición para que $d = \text{mcd}(a, b, c)$.

   Por la segunda condición, tenemos que $\forall z \in A$ tal que $z|\,\text{mcd}(a, b) \wedge z|c$, se tiene que $z|d$. Como $z|\,\text{mcd}(a, b)$, por la transitividad se tiene que $z|a$ y $z|b$, por lo que $\forall z \in A$ tal que $z|a \wedge z|b \wedge z|c$, se tiene que $z|d$. Por tanto, se tiene

también la segunda condición y tenemos que $d = \mathrm{mcd}(a, b, c)$.

Una vez demostrada la primera igualdad, para la segunda tenemos que:

$$\mathrm{mcd}(a, b, c) = \mathrm{mcd}(b, c, a) = \mathrm{mcd}(\mathrm{mcd}(b, c), a) = \mathrm{mcd}(a, \mathrm{mcd}(b, c))$$

5. $\mathrm{mcd}(ac, bc) = \mathrm{mcd}(a, b)c$.

   En el que caso de que alguno de los tres sea nulo es trivial, por lo que supones $a, b, c \neq 0$. Sea $d = \mathrm{mcd}(a, b)$ y $e = \mathrm{mcd}(ac, bc)$. Tenemos que:

$$d = \mathrm{mcd}(a, b) \Longrightarrow \left\{ \begin{array}{ccc} d|a & \Longrightarrow & dc|ac \\ & \wedge & \\ d|b & \Longrightarrow & dc|bc \end{array} \right\} \Longrightarrow dc|e$$

   Como $dc|e$, supongamos $e = dcu$. Además,

$$e = dcu = \mathrm{mcd}(ac, bc) \Longrightarrow \left\{ \begin{array}{ccc} dcu|ac & \Longrightarrow & du|a \\ & \wedge & \\ dcu|bc & \Longrightarrow & du|b \end{array} \right\} \Longrightarrow du|d$$

   Como $du|d$, supongamos ahora $d = duv$. Por tanto, tenemos que $uv = 1$ y, entonces, $u, v \in \mathcal{U}(A)$. Esto implica que $dc \sim e = \mathrm{mcd}(ac, bc)$, y como el mcd es único salvo asociados, tenemos la igualdad pedida.

6. Si $\mathrm{mcd}(a, b) = d$ y $a = da',\ b = db'$, entonces $\mathrm{mcd}(a', b') = 1$.

$$d = \mathrm{mcd}(a, b) = \mathrm{mcd}(a'd, b'd) = \mathrm{mcd}(a', b')d \overset{\mathrm{DI}}{\Longrightarrow} 1 = \mathrm{mcd}(a', b')$$

7. Si $a|bc \ \wedge\ \mathrm{mcd}(a, b) = 1$, entonces $a|c$.

   Tenemos que $a|bc$ implica que $\exists t \in A \mid bc = at$. Entonces:

$$c = c \cdot 1 = c \cdot \mathrm{mcd}(a, b) = \mathrm{mcd}(ac, bc) = \mathrm{mcd}(ac, at) = a \cdot \mathrm{mcd}(c, t) \Longrightarrow a|c$$

8. Si $\mathrm{mcd}(a, b) = 1 \ \wedge\ a|c \ \wedge\ b|c$, entonces $ab|c$.

   Como $b|c$, $\exists x \in A \mid c = bx$. Como $a|bx$ y $\mathrm{mcd}(a, b)$, por la propiedad anterior tenemos que $a|x$, es decir, $\exists y \in A \mid x = ay$. Por tanto, tenemos que $c = aby$, por lo que $ab|c$.

9. $\mathrm{mcd}(a, b) = 1 \ \wedge\ \mathrm{mcd}(a, c) = 1 \Longleftrightarrow \mathrm{mcd}(a, bc) = 1$.

   $\Longrightarrow$) Tenemos que $c = c\,\mathrm{mcd}(a, b) = \mathrm{mcd}(ac, bc)$. Entonces:

$$1 = \mathrm{mcd}(a, c) = \mathrm{mcd}(a, \mathrm{mcd}(ac, bc)) = \mathrm{mcd}(\mathrm{mcd}(a, ac), bc) = \mathrm{mcd}(a, bc)$$

   $\Longleftarrow$) Partimos de que:

$$1 = \mathrm{mcd}(a, bc) = \mathrm{mcd}(\mathrm{mcd}(a, ac), bc) = \mathrm{mcd}(a, \mathrm{mcd}(ac, bc)) = \mathrm{mcd}(a, \mathrm{mcd}(a, b)c)$$

   Como $\mathrm{mcd}(a, b)$ es un divisor común a a y a $\mathrm{mcd}(a, b)c$, tenemos que $\mathrm{mcd}(a, b)$ es un divisor de 1; es decir, una unidad. Por tanto, $\mathrm{mcd}(a, b) = 1$. De la primera igualdad deducimos entonces que $1 = \mathrm{mcd}(a, \mathrm{mcd}(a, b)c) = \mathrm{mcd}(a, c)$.

10. $\mathrm{mcd}(a,b) = \mathrm{mcd}(a-qb,b) \ \ \forall q \in A$.

    Veamos que $Div(a) \cap Div(b) = Div(a-qb) \cap Div(b)$. Demostramos por doble inclusión:

    - Sea $c \in A$ tal que $c|a \wedge c|b$. Entonces, por las propiedades de la divisibilidad tenemos que $c|a-qb \wedge c|b$. Por tanto, la primera inclusión se tiene.
    - Sea $c \in A$ tal que $c|a-qb \wedge c|b$. Entonces, se tiene que $c|(a-qb)+qb$; es decir, $c|a$. Se tiene por tanto la otra inclusión.

    Como tienen los mismos divisores, tienen el mismo mcd.

11. Sea $p \in A$ irreducible. Entonces, $\mathrm{mcd}(p,a) = \begin{cases} p & \text{si} \quad p|a, \\ 1 & \text{si} \quad p \nmid a. \end{cases}$

    Para demostrarlo, realizamos la siguiente división de casos:

    - Si $p|a \overset{3)}{\Longrightarrow} \mathrm{mcd}(p,a) = p$.
    - Si $p \nmid a$, supongamos que $c = \mathrm{mcd}(p,a)$. Por las propiedades del mcd, ha de cumplirse que $c|p$. No obstante, por ser p irreducible tenemos que $c \in \mathcal{U}(A) \vee c = up, \ u \in \mathcal{U}(A)$.
      - Si $c \in \mathcal{U}(A) \Longrightarrow c = 1$, ya que el mcd es único salvo asociados.
      - Si $c = up \mid u \in \mathcal{U}(A)$, tenemos que $p|c$. Por ser $c = \mathrm{mcd}(p,a)$, también $c|a$. Por tanto, por la transitividad de la divisibilidad se tiene que $p|a$, por lo que llegamos a una contradicción.

      Por tanto, estamos en el primer caso y $\mathrm{mcd}(a,p) = 1$.

Ejemplo. Veamos en este ejemplo que en $\mathbb{Z}[\sqrt{-5}]$, $\nexists \, \mathrm{mcd}(2+2\sqrt{-5}, 6)$.

Es importante recordar que $\mathcal{U}(\mathbb{Z}[\sqrt{-5}]) = \{-1, 1\}$. Para demostrar lo pedido, vamos a ver previamente algunos resultados:

1. 3 es irreducible en $\mathbb{Z}[\sqrt{-5}]$:

   Sabemos que $3 \neq 0 \wedge 3 \notin \mathcal{U}(\mathbb{Z}[\sqrt{-5}])$, por lo que puede ser irreducible. Veamos cuáles son sus divisores. Sea $\alpha \in \mathbb{Z}[\sqrt{-5}] \mid \alpha|3 \Longrightarrow \exists \beta \in \mathbb{Z}[\sqrt{-5}] \mid 3 = \alpha \cdot \beta$. Por tanto, aplicando la norma, tenemos que:

   $$N(3) = 9 = N(\alpha)N(\beta)$$

   Veamos las distintas posibilidades que hay:

   - Si $N(\alpha) = 1 \ \wedge \ N(\beta) = 9$, entonces $\alpha \in \mathcal{U}(\mathbb{Z}[\sqrt{-5}])$.
   - Si $N(\alpha) = 3 = N(\beta)$, tenemos que $a^2 + 5b^2 = 3$, con $a, b \in \mathbb{Z}$. Por tanto, como no es posible encontrar a, b, entonces es una contradicción, no es posible.
   - Si $N(\alpha) = 9 \ \wedge \ N(\beta) = 1$, entonces $\beta \in \mathcal{U}(\mathbb{Z}[\sqrt{-5}])$, y como $3 = \alpha\beta$, entonces $\alpha \sim 3$

   Por tanto, sus únicos divisores son los triviales y, por tanto, el 3 es irreducible.

2. Usando la propiedad 11), se tiene que $\exists \operatorname{mcd}(3, 1+\sqrt{-5}) = 1$ porque 3 es irreducible y $3 \not| 1+\sqrt{-5}$. Veamos esto último.

   Si 3 fuese divisor de $1+\sqrt{-5}$, entonces $N(3) = 9$ sería un divisor de $N(1+\sqrt{-5}) = 6$ en $\mathbb{Z}$, pero sabemos que, en $\mathbb{Z}$, $9 \not| 6$, por lo que es una contradicción.

Demostramos ahora lo pedido mediante reducción al absurdo. Supongamos que $\exists \operatorname{mcd}(2+2\sqrt{-5}, 6)$:

$$\operatorname{mcd}(2+2\sqrt{-5}, 6) = 2 \operatorname{mcd}(1+\sqrt{-5}, 3) = 2 \text{ por ser 3 irreducible.}$$

No obstante, no verifica la segunda condición del mcd, ya que $1+\sqrt{-5} | 2+2\sqrt{-5}$ y $1+\sqrt{-5} | 6$. Esto se debe a que:

$$2+2\sqrt{-5} = 2(1+\sqrt{-5}) \qquad 6 = (1+\sqrt{-5})(1-\sqrt{-5})$$

Sin embargo, $1+\sqrt{-5} \not| 2$, porque $N(1+\sqrt{-5}) = 6 \not| N(2) = 4$.
Por tanto, tenemos que $\nexists \operatorname{mcd}(2+2\sqrt{-5}, 6)$.

Definición 3.10 (Ideal)**.** Sea A un anillo conmutativo, un subconjunto $I \subseteq A$, con $I \neq \emptyset$, diremos que es un **ideal** de A si verifica:

1. Es cerrado para la suma: $\forall x, y \in I \Longrightarrow x+y \in I$.

2. Es cerrado para múltiplos: $\forall x \in I \ \forall a \in A \Longrightarrow ax \in I$.

Teorema 3.27 (Ideal principal)**.** *Sea A un anillo conmutativo y $m \in A$. Definimos el **ideal principal generado por el elemento** m como el ideal:*

$$I = mA := \{ma \mid a \in A\}$$

Demostración. Veamos que mA es un ideal:

1. Sea $x, y \in mA$. Entonces, $\exists a, b \in A \mid x = ma \ \wedge \ y = mb$. Por tanto,

   $$x + y = ma + mb = m(a+b) \in mA$$

2. Sea $x \in mA$. Entonces, $\exists a \in A \mid x = am$. Veamos que es cerrado para el producto:

   $$bx = bam = m(ab) \in mA, \qquad \forall b \in A$$

□

Notemos que:

- Si $m = 0 \Longrightarrow 0A = \{0\}$, es un ideal trivial de A.
- Si $m = 1 \Longrightarrow 1A = A$, es un ideal.
- Si I es cualquier otro ideal de A, entonces $\{0\} \subseteq I \subseteq A$.

Teorema 3.28. *Si A es un DE, entonces todo ideal de A es principal.*

Demostración. Sea $\phi : A \setminus \{0\} \to \mathbb{N}$ la función euclídea de A y I un ideal de A. Si $I = \{0\}$ tenemos que $I = 0A$ y está demostrado. Consideramos por tanto $I \neq \{0\}$, y definimos $X = \{\phi(x) \mid x \in I \ \wedge \ x \neq 0\} \subseteq \mathbb{N}$.

Como $\mathbb{N}$ es bien ordenado, sabemos que $\exists\, \text{mín}(X)$. Sea $m \in I \mid \phi(m) = \text{mín}(X)$. Veamos que $mA = I$ (sabemos que $m \neq 0$ porque $m \in X$):
Como $m \in I$, entonces por ser I un ideal tenemos $ma \in I \ \forall a \in A$. Entonces, $mA \subseteq I$. Veamos la otra inclusión:

Sea $x \in I$, sabemos que $\exists q, r \in A \mid x = mq + r$ con $r = 0 \ \vee \ \phi(r) < \phi(m)$. Entonces:

- Supongamos que $r \neq 0$. Entonces, como $\phi(r) < \phi(m)$ y $\phi(m) = \text{mín}(X)$, tenemos que $r \notin I$.

  Además, por ser $r \neq 0$, tenemos que $r = x - mq$, que por las propiedades de los ideales tenemos que $r \in I$. Por tanto, llegamos a una contradicción.

- Supongamos $r = 0$, es decir, $x = mq \in mA$.

Por tanto, al ser el primer caso una contradicción, tenemos el segundo caso. Por tanto, por doble inclusión, tenemos que $I = mA$. □

Corolario 3.28.1. *Sea A un DE y $a, b \in A$. Entonces $\exists\, \text{mcd}(a, b)$.*
Además, si $d = \text{mcd}(a, b)$, entonces $\exists u, v \in A$ tal que

$$\text{mcd}(a, b) = d = au + bv \tag{3.1}$$

*A u, v se les llama **coeficientes de Bezout**, siendo la Ecuación 3.1 la **identidad de Bezout**.*

Demostración. Consideramos $I = \{ax + by \mid x, y \in A\}$ y tenemos que $a, b \in I$, puesto que $\left\{ \begin{array}{l} a = a \cdot 1 + b \cdot 0 \in I \\ b = a \cdot 0 + b \cdot 1 \in I \end{array} \right\}$. Veamos que I es un ideal de A.

1. Sean $w = ax_1 + by_1, z = ax_2 + by_2 \in A$. Entonces:

$$w + z = ax_1 + by_1 + ax_2 + by_2 = a(x_1 + x_2) + b(y_1 + y_2) \in I$$

2. Sea $w = ax + by$, $c \in A$. Entonces:

$$w = c(ax + by) = cax + cby = a(cx) + b(cy) \in I$$

Entonces, como A es un Dominio Euclídeo, por el Teorema 3.28, tenemos que $\exists d \in I \mid I = dA$. Notemos que $d \in I$, por lo que $\exists u, v \in A \mid d = au + bv$. Queda por tanto demostrada la Identidad de Bezout. Veamos ahora que $d = \text{mcd}(a, b)$:

1. Como $a, b \in I = dA = \{dx \mid x \in A\}$, entonces $\exists a', b' \in A \mid a = da' \ \wedge \ b = db'$, por lo que $d|a \ \wedge \ d|b$.

2. Sea $c \in A \mid c|a \ \wedge \ c|b \Longrightarrow \exists a'', b'' \in A \mid a = ca'' \ \wedge \ b = cb''$

$$d = au + bv = ca''u + cb''v = c(a''u + b''v) \Longrightarrow c|d$$

Por tanto, tenemos que $d = \text{mcd}(a, b)$. □

3.4.1. Algoritmo extendido de Euclídes

Sea A un DE con $a,\ b \in A$ siendo $\phi : A \setminus \{0\} \to \mathbb{N}$ la función euclídea de A. Nuestro objetivo es calcular $\text{mcd}(a,b)$ y $u, v \in A \mid \text{mcd}(a,b) = au + bv$, los coeficientes de Bezout de a y b.

Realizamos la siguiente división por casos:

1. Si ambos son cero: $a = b = 0 \Longrightarrow \text{mcd}(a,b) = 0$ y $0 = 0 \cdot u + 0 \cdot v \ \ \forall u, v \in A$.

2. Si uno es cero (por ejemplo, $a = 0$), entonces $\text{mcd}(0,b) = b$ y $b = a \cdot 0 + b \cdot 1$.

3. Si $a \neq 0 \neq b$ y suponemos (lo cual no es restrictivo ya que $\text{mcd}(a,b) = \text{mcd}(b,a)$) $\phi(a) \geqslant \phi(b)$:

   Construimos una sucesión $r_1, r_2, \ldots, r_i$ de elementos de A de forma recurrente. Partimos de

   $$r_1 = a \ \wedge \ r_2 = b$$

   Para el resto de valores, si $r_i \neq 0$, entonces:

   $$r_{i+1} = R(r_{i-1}; r_i) \ \ \forall i \in \{2, \ldots, n\}$$

   Consideramos ahora la sucesión $\{\phi(r_i)\}$. Tenemos que es estrictamente decreciente, ya que por la definición de función euclídea:

   $$\phi(r_1) \geqslant \phi(r_2) > \phi(r_3) > \ldots > \phi(r_i) > \ldots$$

   Por tanto, al ser una sucesión en $\mathbb{N}$ estrictamente decreciente y minorada por el 0, tenemos que $\exists n \in \mathbb{N} \mid r_{n+1} = 0$. Demostremos a continuación que $r_n = \text{mcd}(a,b)$, es decir, que $\text{mcd}(a,b)$ es el último resto no nulo. Para ello, demostramos por inducción que $\forall i \in \mathbb{N}$ se tiene que $\text{mcd}(a,b) = \text{mcd}(r_i, r_{i+1})$:

   - Si $i = 1 \Longrightarrow r_1 = a,\ r_2 = b \Longrightarrow \text{mcd}(a,b) = \text{mcd}(a,b)$, Cierto.
   - Supongamos que $i > 1$ y que $\text{mcd}(a,b) = \text{mcd}(r_{i-1}, r_i)$:

     $$\text{mcd}(a,b) \overset{HI}{=} \text{mcd}(r_{i-1}, r_i) \overset{10)}{=} \text{mcd}(r_{i-1} - r_i q_i, r_i) = \text{mcd}(r_{i+1}, r_i) = \text{mcd}(r_i, r_{i+1})$$

   Por tanto, para $i = n$ tenemos que:

   $$\text{mcd}(a,b) = \text{mcd}(r_n, r_{n+1}) = \text{mcd}(r_n, 0) = r_n$$

   es decir, que el mcd es el último resto no nulo.

   A continuación, veamos que $\forall i \in \{1, \ldots, n\}$, $\exists u_i, v_i \mid r_i = au_i + bv_i$. Hacemos inducción en i:

   - Si $i = 1 \Longrightarrow r_1 = a \Longrightarrow u_1 = 1 \ \wedge \ v_1 = 0$
   - Si $i = 2 \Longrightarrow r_2 = b \Longrightarrow u_2 = 0 \ \wedge \ v_2 = 1$

- Supongamos que $i > 1$ y que $r_{i-1} = au_{i-1} + bv_{i-1} \ \wedge \ r_i = au_i + bv_i$:

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

  Por tanto, $u_{i+1} = u_{i-1} - q_i u_i \ \wedge \ v_{i+1} = v_{i-1} - q_i v_i$.

En particular, $\text{mcd}(a, b) = r_n = au_n + bu_n$.

Ejemplo. Trabajamos en $\mathbb{Z}$ y queremos hallar $\text{mcd}(80, 30)$ y su identidad de Bezout.

i	r_i	u_i	v_i	
1	80	1	0	
2	30	0	1	$80 = 30 \cdot 2 + 20$
3	20	1	-2	$30 = 20 \cdot 1 + 10$
4	10	-1	3	$20 = 10 \cdot 2 + 0$
5	0			

Por tanto, tenemos que $\text{mcd}(80, 30) = 10 = -1 \cdot 80 + 3 \cdot 30$.

Las operaciones para hallar los coeficientes de bezout han sido:

$$u_3 = u_1 - q_2 u_2 = 1 - 2 \cdot 0 = 1 \qquad u_4 = u_2 - q_3 u_3 = 0 - 1 \cdot 1 = -1$$
$$v_3 = v_1 - q_2 v_2 = 0 - 2 \cdot 1 = 2 \qquad v_4 = v_2 - q_3 v_3 = 1 - 1 \cdot (-2) = 3$$

3.5. Ecuaciones Diofánticas

Definición 3.11 (Ecuación diofántica)**.** Llamamos **ecuación diofántica** en un DI A a cualquier ecuación del tipo:

$$ax + by = c, \qquad a, b, c \in A, \ a, b \neq 0$$

siendo x e y las incógnitas a buscar.

Decimos que una solución a la ecuación diofántica anterior es $(x_0, y_0) \in A \times A$ si:

$$ax_0 + by_0 = c$$

Teorema 3.29. *Sea A un DE y consideramos la ecuación diofántica:*

$$ax + by = c$$

Con $a, b, c \in A \mid a, b \neq 0$ y con incógnitas x e y. Sea $d = \text{mcd}(a, b)$:

1. *La ecuación tiene solución $\iff d|c$.*
2. *Si (x_0, y_0) es una solución particular de la ecuación, entonces las demás soluciones son del tipo:*

$$x = x_0 + k \cdot \frac{b}{d} \qquad y = y_0 - k \cdot \frac{a}{d} \qquad \forall k \in A$$

Demostración. Sea $d = \text{mcd}(a, b)$, y sean $a = da'$, $b = db'$, con $a', b' \in A$ tal que $\text{mcd}(a', b') = 1$. Entonces:

1. Demostramos mediante doble implicación:

   $\Longrightarrow$) Supongamos que $\exists x_0, y_0 \in A \mid ax_0 + by_0 = c$. Entonces:

   $$c = da'x_0 + db'y_0 = d(a'x_0 + b'y_0) \Longrightarrow d|c$$

   $\Longleftarrow$) Supongamos que $d|c \Longrightarrow \exists c' \in A \mid c = dc'$. Entonces:

   $$ax + by = c \Longleftrightarrow da'x + db'y = dc' \Longleftrightarrow a'x + b'y = c'$$

   Como $\text{mcd}(a', b') = 1$, buscamos $u, v \in A \mid 1 = a'u + b'v$ con $u, v \in A$ los coeficientes de Bezout.

   $$1 = a'u + b'v \Longleftrightarrow c' = a'uc' + b'vc' \Longrightarrow (x_0 = uc', y_0 = vc') \text{ es solución.}$$

2. Como la ecuación tiene solución $\Longrightarrow d|c \Longrightarrow \exists c' \mid c = dc'$:

   $$ax + by = c \Longleftrightarrow da'x + db'y = dc' \Longleftrightarrow a'x + b'y = c'$$

   Sea (x_0, y_0) una solución, y consideramos $k \in A$:

   $$a'(x_0 + kb') + b'(y_0 - ka') = a'x_0 + ka'b' + b'y_0 - ka'b' = a'x_0 + b'y_0 = c'$$

   Por tanto, $(x_0 + kb', y_0 - ka')$ es solución. Falta ver que no hay más soluciones.

   Sea (x_1, y_1) otra solución y veamos que es de la forma anterior:

   $$a'x_1 + b'y_1 = c' = a'x_0 + b'y_0 \Longrightarrow a'(x_1 - x_0) = b'(y_0 - y_1)$$

   Entonces, sabiendo que $\text{mcd}(a', b') = 1$, tenemos que:

   $$b'|a'(x_1 - x_0) \overset{\text{mcd}(a',b')=1}{\Longrightarrow} b'|x_1 - x_0 \Longrightarrow \exists k \in A \mid x_1 - x_0 = kb' \Longrightarrow x_1 = x_0 + kb'$$
   $$a'|b'(y_0 - y_1) \overset{\text{mcd}(a',b')=1}{\Longrightarrow} a'|y_0 - y_1 \Longrightarrow \exists h \in A \mid y_0 - y_1 = ha' \Longrightarrow y_1 = y_0 - ha'$$

   Nos falta ver que $k = h$. Como A es un DI, tenemos que:

   $$a'(x_1 - x_0) = b'(y_0 - y_1) \Longrightarrow a'kb' = b'ha' \Longleftrightarrow k = h$$

   Por tanto, las soluciones son del tipo:

   $$(x_0 + kb', y_0 - ka') = \left(x_0 + k \cdot \frac{b}{d}, y_0 - k \cdot \frac{a}{d}\right)$$

□

Ejemplo. Consideramos $A = \mathbb{Z}[i]$. Se pide resolver:

$$(-2 + 3i)x + (1 + i)y = 1 + 11i$$

En primer lugar, calculamos el mcd para ver si la ecuación diofántica tiene solución. Para ello, aplicamos el algoritmo extendido de Euclídes. Para ello, en primer lugar tengo que dividir r_1 entre r_2 en $\mathbb{Z}[i]$. En $\mathbb{Q}[i]$:

$$\frac{-2+3i}{1+i} = \frac{(-2+3i)(1-i)}{2} = \frac{1}{2} + \frac{5}{2}i$$

Para dividir en $\mathbb{Z}[i]$, elegimos q_1, q_2 tal que $\left|\frac{1}{2} - q_1\right| \leqslant \frac{1}{2} \ \wedge \ \left|\frac{5}{2} - q_2\right| \leqslant \frac{1}{2}$.

Sean $q_1 = 1 \ \wedge \ q_2 = 2 \Longrightarrow q = 1 + 2i \ \wedge \ r_3 = -2 + 3i - (1+2i)(1+i) = -1$. Por tanto, el algoritmo extendido de Euclídes queda de la siguiente forma:

i	r_i	u_i	v_i
1	$-2+3i$	1	0
2	$1+i$	0	1
3	-1	1	$-1-2i$
4	0		

Entonces, tenemos el mcd:

$$\mathrm{mcd}(-2+3i, 1+i) = -1 \overset{-1\sim 1}{\Longleftrightarrow} \mathrm{mcd}(-2+3i, 1+i) = 1$$

Como $1|(1+11i) \Longrightarrow$ la ecuación tiene solución. Para calcularla, partimos de la identidad de Bezout:

$$\begin{gathered} -1 = (-2+3i)\cdot 1 + (1+i)(-1-2i) \\ 1 = (-2+3i)(-1) + (1+i)(1+2i) \\ (1+11i) = (-2+3i)(-1-11i) + (1+i)(1+2i)(1+11i) \\ (1+11i) = (-2+3i)(-1-11i) + (1+i)(-21+13i) \end{gathered}$$

Por tanto, una solución particular es $x_0 = -1-11i$, $y_0 = -21+13i$. La solución general es:

$$\begin{cases} x = -1 - 11i + \alpha(1+i) \\ y = -21 + 13i - \alpha(-2+3i) \end{cases} \qquad \forall \alpha \in \mathbb{Z}[i]$$

3.6. Mínimo Común Múltiplo

Definición 3.12 (Mínimo común múltiplo)**.** Sea A un DI y $a, b \in A$. Un elemento $m \in A$ diremos que es un **mínimo común múltiplo** (abreviado como mcm) y notado $m = \mathrm{mcm}(a,b)$ si verifica:

1. $a|m \ \wedge \ b|m$,
2. $\forall c \in A$ tal que $a|c \ \wedge \ b|c \Longrightarrow m|c$.

Observación. No siempre existe el mínimo común múltiplo de dos elementos.

Además, si existe no es único (lo es cualquier asociado a él, únicamente). Para verlo, si $m = \mathrm{mcm}(a,b)$, consideramos mu, con $u \in \mathcal{U}(A)$. Entonces:

1. Como $m|mu$, y se tiene que $a|m \wedge b|m$, por la transitividad, se tiene que $a|mu$ y $b|mu$.

2. Si $c \in A$ cumple que $a|c \wedge b|c$, entonces $m|c$; y la transitividad afirma que $mu|c$ al tener que $mu|m$.

Por tanto, hemos visto que $mu = \text{mcm}(a, b)$. Tenemos que el mcm de dos elementos, si existe, es único salvo asociados. Hablaremos simplemente de mcm de a y b.

Definición 3.13 (Mínimo común múltiplo generalizado)**.** Sea A un DI y $a_1, a_2, \ldots, a_n \in A$, $(n \geqslant 2)$, un mínimo común múltiplo de $a_1, a_2, \ldots, a_n$, notado $\text{mcm}(a_1, a_2, \ldots, a_n)$ es $m \in A$ tal que verifica:

1. $a_i|m \ \ \forall i \in \{1, \ldots, n\}$,
2. Si $c \in A$ tal que $a_i|c \ \ \forall i \in \{1, \ldots, n\} \Longrightarrow m|c$.

Propiedades del mcm. Sea A DI, supuesta la existencia de los mcm que intervienen, tenemos que:

1. $\text{mcm}(a, b) = \text{mcm}(b, a)$. En general:

   $$\text{mcm}(a_1, \ldots, a_i, a_{i+1}, a_n) = \text{mcm}(a_1, \ldots, a_{i+1}, a_i, \ldots, a_n), \ \ n \geqslant 2, \ i \in \{1, \ldots, n\}$$

   La demostración es trivial, ya que en la definición no se establece ningún orden.

2. Si $a \sim a' \Longrightarrow \text{mcm}(a, b) = \text{mcm}(a', b)$.

   Sea $m = \text{mcm}(a, b)$. Entonces, $a|m$. Además, por ser $a \sim a'$, se tiene que $a'|a$. Por la transitividad, $a'|m$. Además, se tiene también que $b|m$, por lo que la primera condición se tiene.

   Veamos la segunda. Como $a \sim a'$, tenemos que $c|a \Longleftrightarrow c|a'$, por lo que $\forall c \in A$ se tiene que si $c|a' \wedge c|b$, entonces $c|a \wedge c|b$; y por tanto $m|c$. Por tanto, se deduce que $m = \text{mcm}(a', b)$.

3. $\text{mcm}(a, b) = a \Longleftrightarrow b|a$. En particular: $\text{mcm}(a, 0) = 0 \ \wedge \ \text{mcm}(a, 1) = 1$.

   $\Longrightarrow$) $\text{mcm}(a, b) = a \Longrightarrow a|a \wedge b|a$.

   $\Longleftarrow$) Partimos de que $b|a$. Además, por reflexividad, tenemos que $a|a$. Entonces, se tiene la primera condición.

   Además, como $\forall c \in A \mid a|c \wedge b|c$ se tiene que $a|c$, tenemos la segunda condición. Por tanto, $a = \text{mcm}(a, b)$.

4. $\text{mcm}(\text{mcm}(a, b), c) = \text{mcm}(a, b, c) = \text{mcm}(a, \text{mcm}(b, c))$.

   Demostramos en primer lugar la primera igualdad. Sea $m = \text{mcm}(\text{mcm}(a, b), c)$. Por tanto, $\text{mcm}(a, b)|m \wedge c|m$. Además, como $a|\text{mcm}(a, b) \wedge b|\text{mcm}(a, b)$; por la transitividad se tiene que $a|m \wedge b|m$. Por tanto, se cumple la primera condición para que $m = \text{mcm}(a, b, c)$.

   Por la segunda condición, tenemos que $\forall z \in A$ tal que $\text{mcm}(a, b)|z \wedge c|z$, se tiene que $m|z$. Como $\text{mcm}(a, b)|z$, por la transitividad se tiene que $a|z \wedge b|z$. Por tanto, como $\forall z \in A$ tal que $a|z \wedge b|z \wedge c|z$ se tiene que $m|c$; entonces

tenemos la segunda condición y $m = \text{mcm}(a, b, c)$.

Una vez demostrada la primera igualdad, para la segunda tenemos que:

$$\text{mcm}(a, b, c) = \text{mcm}(b, c, a) = \text{mcm}(\text{mcm}(b, c), a) = \text{mcm}(a, \text{mcm}(b, c))$$

5. $\text{mcm}(ac, bc) = \text{mcm}(a, b)c$.
   Se deduce de forma directa de la definición. Se deja como ejercicio.
6. $\text{mcd}(a, b) = 1 \Longrightarrow \text{mcm}(a, b) = ab$.
   Veamos las dos condiciones:
   a) Claramente $a|ab \ \wedge \ b|ab$.
   b) Sea $c \in A$ tal que $a|c \ \wedge \ b|c \underset{\text{mcd}(a,b)=1}{\overset{8)}{\Longrightarrow}} ab|c$.

Teorema 3.30. *Sea A un DE y a, $b \in A$. Entonces $\exists\, \text{mcm}(a, b)$. Se verifica además que*

$$\text{mcm}(a, b)\,\text{mcd}(a, b) = ab$$

Demostración. Sean $I_1 = aA$, $I_2 = bA$. Entonces, $I = I_1 \cap I_2$ es un ideal de A (veámoslo):

1. Cerrado para sumas:
$$\forall w, z \in I \Longrightarrow \left\{ \begin{array}{rcl} w, z \in I_1 & \Longrightarrow & w + z \in I_1 \\ w, z \in I_2 & \Longrightarrow & w + z \in I_2 \end{array} \right\} \Longrightarrow w + z \in I$$
2. Cerrado para múltiplos:
$$\forall w \in I \ \forall c \in A \Longrightarrow \left\{ \begin{array}{rcl} w \in I_1 & \Longrightarrow & wc \in I_1 \\ w \in I_2 & \Longrightarrow & wc \in I_2 \end{array} \right\} \Longrightarrow wc \in I$$

Como A es DE $\Longrightarrow \exists m \in A \mid I = mA$. Veamos que $m = \text{mcm}(a, b)$:

1. Como $m \in I \Longrightarrow \left\{ \begin{array}{rcl} m \in I_1 = aA & \Longrightarrow & a|m \\ m \in I_2 = bA & \Longrightarrow & b|m \end{array} \right\}$
2. Sea $c \in A$ tal que $a|c \ \wedge \ b|c \Longrightarrow \exists x, y \in A \mid c = ax \ \wedge \ c = bx$. Entonces, tenemos que $c \in aA = I_1 \ \wedge \ c \in bA = I_2 \Longrightarrow c \in I = mA \Longrightarrow m|c$. Por tanto, $m = \text{mcm}(a, b)$.

Veamos ahora la relación entre el mcd y el mcm dada. Si $d = \text{mcd}(a, b)$, tenemos que $\exists a', b' \in A \mid a = da' \ \wedge \ b = db'$ con $\text{mcd}(a', b') = 1$. Por la propiedad 6), tenemos que $\text{mcm}(a', b') = a'b'$. Por tanto:

$$\begin{aligned} \text{mcm}(a, b)\,\text{mcd}(a, b) = \text{mcm}(da', db')\,\text{mcd}(da', db') = d \cdot \text{mcm}(a', b') \cdot d \cdot \text{mcd}(a', b') = \\ = d^2 \cdot a'b' = da' \cdot db' = ab \end{aligned}$$

□

Corolario 3.30.1. *Consecuencia del Corolario 3.28.1 y del Teorema 3.30.*

Sea A un DE con $a,\ b \in A$. Consideramos los ideales $I_1 = aA$ y $I_2 = bA$. Entonces:

$$I = I_1 + I_2 = \{ax + by \mid x, y \in A\}$$
$$J = I_1 \cap I_2 = \{abx \mid x \in A\}$$

son ideales. Se verifica que:

$$I = \text{mcd}(a, b)A \qquad\qquad J = \text{mcm}(a, b)A$$

Notemos que para demostrar que I y J son ideales no es necesario imponer que A sea DE (lo es para demostrar que son principales), nos es suficiente con que sea un anillo conmutativo.

3.7. Congruencias

Definición 3.14 (Elementos congruentes)**.** Sea A un anillo conmutativo (trabajaremos con DI) y sea $I \subseteq A$ un ideal. Dos elementos $a, b \in A$ diremos que son **congruentes módulo** I, notado $a \equiv b \mod (I)$ ó $a \equiv_I b$ si:

$$a - b \in I$$

Notación. Sea I el ideal generado por $m \in A$; es decir, $I = mA$. Entonces si queremos decir que $a \equiv b \mod (mA)$, podremos notar:

$$a \equiv b \mod (m) \quad \text{ó} \quad a \equiv_m b$$

Por tanto:

$$a \equiv b \mod (m) \iff a - b \in mA \iff m | a - b \iff \exists k \in A \mid a - b = km \iff$$
$$\iff \exists k \in A \mid a = km + b \quad \text{es decir, } b \text{ es un resto de dividir } a \text{ entre } m.$$

Notemos que si $A = \mathbb{Z}$ y $m \geqslant 2$. Entonces:

$$a \equiv b \mod (m) \iff aR_m b$$

Propiedades de las congruencias. Sean $a, b, c, d \in A$ con A anillo conmutativo, y sea I un ideal. Entonces:

1. $\cdot \equiv \cdot \mod (I)$ es una relación de equivalencia.

   Demostramos las tres condiciones:

   - Reflexividad: $a \equiv a \mod (I) \iff 0 \in I$, lo cual es cierto.
   - Simetría: Si $a \equiv b \mod (I)$, entonces $a - b \in I$. Por tanto, como es cerrado para múltiplos, tenemos que $b - a \in I$, por lo que $b \equiv a \mod (I)$.
   - Transitividad: Si $a \equiv b \mod (I) \wedge \equiv c \mod (I)$, tenemos que $a - b, b - c \in I$. Entonces, $a - b + b - c = a - c \in I$, por ser el ideal cerrado para sumas. Por tanto, $a \equiv c \mod (I)$.

2. $a \equiv 0 \mod (I) \iff a \in I$.

$$a \equiv 0 \mod (I) \iff a - 0 \in I \iff a \in I$$

3. Si $a \equiv b \mod (I) \iff \begin{cases} a + c \equiv b + c \mod (I) \\ ac \equiv bc \mod (I) \end{cases} \quad \forall c \in A.$

Veamos en primer lugar el resultado para la suma:

$$a \equiv b \mod (I) \iff a - b \in I \iff a + c - c - b \in I \ \ \forall c \in A \iff$$
$$\iff (a + c) - (b + c) \in I \ \ \forall c \in A \iff a + c \equiv b + c \mod (I) \ \ \forall c \in A$$

Veamos ahora el resultado para el producto:

$$a \equiv b \mod (I) \iff a - b \in I \implies c(a - b) \in I \ \ \forall c \in A \iff$$
$$\iff ac - bc \in A \ \ \forall c \in A \iff ac \equiv bc \mod (I) \ \ \forall c \in A$$

4. Si $a \equiv b \mod (I) \ \wedge \ c \equiv d \mod (I) \implies \begin{cases} a + c \equiv b + d \mod (I) \\ ac \equiv bd \mod (I) \end{cases}$.

Veamos en primer lugar el resultado para la suma:

$$\left.\begin{array}{ll} a \equiv b & \mod (I) \\ c \equiv d & \mod (I) \end{array}\right\} \iff \left\{\begin{array}{l} a - b \in I \\ c - d \in I \end{array}\right\} \implies (a - b) + (c - d) \in I \implies$$
$$\implies (a + c) - (b + d) \in I \iff a + c \equiv b + d \mod (I)$$

Veamos ahora el resultado para el producto:

$$\left.\begin{array}{ll} a \equiv b & \mod (I) \\ c \equiv d & \mod (I) \end{array}\right\} \iff \left\{\begin{array}{l} a - b \in I \\ c - d \in I \end{array}\right\} \implies \left\{\begin{array}{l} c(a - b) \in I \\ b(c - d) \in I \end{array}\right\} \implies$$
$$\implies c(a-b)+b(c-d) \in I \iff ac-bc+bc-bd \in I \iff ac-bd \in I \iff ac \equiv bd \mod (I)$$

A partir de ahora, sea A un DE y sea $I = mA$ con $m \in A \mid m \neq 0$:

5. Sea r un resto de dividir a por m es decir, entonces $a \equiv r \mod (m)$.

Dividimos a entre m: $a = mq + r$ con $r = 0 \ \vee \ \phi(r) < \phi(m)$.

$$a - r = mq \implies a - r \in mA \iff a \equiv r \mod (m)$$

6. $a \equiv b \mod (m) \iff a$ y b tienen el mismo resto al dividirlos entre m.

$\implies$) $a \equiv b \mod (m) \iff a - b \in mA \iff \exists k \in A \mid a - b = km$.
Dividimos b entre m: $b = mq + r$ con $r = 0 \ \vee \ \phi(r) < \phi(m)$, por lo que r es un resto de dividir b entre m.
Como $a - b = km \implies a = b + km \implies a = mq + r + km = m(q + k) + r$ con $r = 0 \ \vee \ \phi(r) < \phi(m)$ por lo que r es un resto de dividir a entre m.

$\Longleftarrow$) Supongamos que $a = mq + r$ con $r = 0 \ \vee \ \phi(r) < \phi(m)$ y $b = mq' + r$. Luego:

$$a-b = mq+r-mq'-r = m(q-q') \Longrightarrow a-b \in mA \Longleftrightarrow a \equiv b \mod (m)$$

7. Si $\left\{ \begin{array}{c} ac \equiv bc \mod (m) \\ \wedge \\ \mathrm{mcd}(c,m) = 1 \end{array} \right\} \Longrightarrow a \equiv b \mod (m)$.

$$ac \equiv bc \mod (m) \Longleftrightarrow ac-bc \in mA \Longleftrightarrow c(a-b) \in mA \Longrightarrow m|c(a-b) \Longrightarrow$$
$$\underset{\mathrm{mcd}(c,m)=1}{\overset{7)}{\Longrightarrow}} m|a-b \Longrightarrow a-b \in mA \Longleftrightarrow a \equiv b \mod (m)$$

Notemos que el recíproco es cierto $\forall c \in A$ sin tener que $\mathrm{mcd}(c,m) = 1$.

8. Sea $c \neq 0$. Entonces $ac \equiv bc \mod (mc) \Longleftrightarrow a \equiv b \mod (m)$.

$$ac \equiv bc \mod (mc) \Longleftrightarrow ac - bc \in mcA \Longleftrightarrow \exists k \in A \mid ac - bc = mck \Longleftrightarrow$$
$$\Longleftrightarrow a - b = mk \Longleftrightarrow a - b \in mA \Longleftrightarrow a \equiv b \mod (m)$$

Cuidado con la propiedad 7: Si $A = \mathbb{Z}$ y queremos simplificar $30 \equiv 6 \mod (8)$:

$$\left. \begin{array}{l} 30 \equiv 6 \mod (8) \\ 30 = 3 \cdot 10 \\ 6 = 3 \cdot 2 \\ \mathrm{mcd}(3,8) = 1 \end{array} \right\} \overset{7)}{\Longrightarrow} 10 \equiv 2 \mod (8)$$

No obstante,

$$\left. \begin{array}{l} 10 \equiv 2 \mod (8) \\ 10 = 2 \cdot 5 \\ 2 = 2 \cdot 1 \\ \mathrm{mcd}(2,8) = 2 \end{array} \right\} \not\Rightarrow 5 \equiv 1 \mod (8)$$

ya que $5 - 1 = 4 \notin 8\mathbb{Z} = \{\ldots, -16, -8, 0, 8, 16, \ldots\}$

Lo que sí podemos hacer es, usando la propiedad 8,

$$\left. \begin{array}{l} 10 \equiv 2 \mod (8) \\ 10 = 2 \cdot 5 \\ 2 = 2 \cdot 1 \\ 8 = 2 \cdot 4 \\ 2 \neq 0 \end{array} \right\} \overset{8)}{\Longrightarrow} 5 \equiv 1 \mod (4)$$

que sí es cierto: $5 - 1 = 4 \in 4\mathbb{Z}$

3.7.1. Ecuaciones de congruencias

Sea A un DE, estamos interesados en resolver en A ecuaciones de la forma:

$$ax \equiv b \mod (m)$$

Con $a, b, m \in A$, $a, m \neq 0$ y x incógnita.

Sabemos por ahora que, si $a = 1$ (o unidad), las soluciones son:

$$x \equiv b \mod (m) \iff x - b \in mA \iff x \in \{b + km \mid k \in A\}$$

Veamos el caso general:

Teorema 3.31. *Sea A un DE, sea una ecuación del tipo:*

$$ax \equiv b \mod (m)$$

Con $a, b, m \in A \mid a, m \neq 0$ y x una incógnita. Sea $d = \mathrm{mcd}(a, m)$. Entonces:

1. *La ecuación tiene solución $\iff d|b$.*
2. *Supongamos que tiene solución $\implies d|b$. Consideramos $b = db'$, $a = da'$, $m = dm'$. Entonces, la ecuación anterior es equivalente (tiene las mismas soluciones) a la ecuación:*

   $$a'x \equiv b' \mod (m')$$

   *que llamaremos **ecuación reducida** de la ecuación primitiva.*
3. *Supongamos que tiene solución y sea x_0 una solución particular. Entonces, la ecuación reducida y la primitiva son equivalentes a la ecuación:*

   $$x \equiv x_0 \mod (m')$$

   Por tanto, las soluciones de la ecuación primitiva son $\{x_0 + km' \mid k \in A\}$.
4. *Supongamos que tiene solución. Entonces, podemos encontrar una solución:*

   $$y_0 \in A \mid y_0 = 0 \ \vee \ \phi(y_0) < \phi(m')$$

   *que llamaremos **solución óptima** de la ecuación. y usaremos para dar el conjunto de soluciones del sistema:*

   $$\{y_0 + km' \mid k \in A\}$$

Demostración. Demostramos cada una de las partes:

1. La ecuación primitiva tiene solución si y solo si:

   $$\begin{aligned}
   &\exists x_0 \in A \mid ax_0 \equiv b \mod (m) \iff \\
   &\quad \iff \exists x_0 \in A \mid ax_0 - b \in mA \iff \exists x_0 \in A \ \wedge \ \exists y_0 \in A \mid ax_0 - b = my_0 \iff \\
   &\quad \iff \exists x_0, y_0 \in A \mid ax_0 - my_0 = b \iff \text{La diofántica } ax - my = b \text{ tiene solución} \iff \\
   &\quad \iff \mathrm{mcd}(a, -m) = \mathrm{mcd}(a, m) | b \iff d|b
   \end{aligned}$$

2. Suponemos que tiene solución; es decir, que $d|b$. Entonces, por lo visto y por ser $d = \mathrm{mcm}(a, m)$, entonces $\exists a', b', m' \in A$ tales que $a = da', b = db', m = dm'$. Entonces:

   $$ax_0 \equiv b \mod (m) \iff da'x_0 \equiv db' \mod (dm') \iff a'x_0 \equiv b' \mod (m')$$

3. Suponemos que tiene solución:

$$ax \equiv b \mod (m) \iff a'x \equiv b' \mod (m') \text{ con } \mcd(a', m') = 1$$

Sabemos por el Corolario 3.28.1 que $\exists u, v \in A \mid 1 = a'u + m'v$. Entonces:

$$1 = a'u+m'v \iff a'u-1 = -m'v \iff a'u \equiv 1 \mod (m') \overset{3)}{\Longrightarrow} a'ub' \equiv b' \mod (m')$$

Por tanto, $x_0 = ub'$ es solución de la ecuación reducida (y por tanto, de la primitiva).

Es claro que $\forall k \in A$, $x_0 + km'$ es una solución, puesto que:

$$a'(x_0+km')-b' = a'x_0+km'a'-b' = \underbrace{a'x_0 - b'}_{k'm'}+km'a' = ka'm'+k'm' = (k'+ka')m' \in m'A$$

Veamos que todas las soluciones son de dicha forma. Sea y_0 otra solución. Entonces:

$$\left.\begin{array}{l} a'y_0 \equiv b' \mod (m') \\ a'x_0 \equiv b' \mod (m') \end{array}\right\} \overset{1)}{\Longrightarrow} \left\{\begin{array}{c} a'y_0 \equiv a'x_0 \mod (m') \\ \mcd(a', m') = 1 \end{array}\right\} \overset{1)}{\Longrightarrow}$$

$$\Longrightarrow y_0 \equiv x_0 \mod (m') \Longrightarrow y_0 \text{ es solucion de } x \equiv x_0 \mod (m')$$

Por tanto, tenemos que la ecuación es equivalente a $x \equiv x_0 \mod (m')$.

4. Sea x_0 una solución. Dividimos x_0 entre m' y obtenemos $x_0 = m'q + y_0$ con $y_0 = 0 \ \vee \ \phi(y_0) < \phi(m')$.

Por la división, tenemos que $x_0 \equiv y_0 \mod (m')$; y sabiendo que $\mcd(a', m') = 1$, tenemos que $a'x_0 \equiv a'y_0 \mod (m')$. Por otro lado, tenemos que x_0 es una solución. Entonces, $a'x_0 \equiv b' \mod (m')$.

De ambas congruencias, por transitividad tenemos que $a'y_0 \equiv b' \mod (m')$, de donde deducimos que y_0 es una solución, la denominada óptima.

□

Ejemplo. Resolver en $\mathbb{Z}$:

1. $60x \equiv 90 \mod (105)$.

Veamos en primer lugar si tiene solución:

$$\mcd(60, 105) = 15 \ \wedge \ 90 = 15 \cdot 6 \Longrightarrow 15|90 \Longrightarrow \text{ Sí tiene solución.}$$

Tenemos que la ecuación reducida es $4x \equiv 6 \mod (7)$, con $\mcd(4, 7) = 1$.

Buscamos los coeficientes de Bezout: $u, v \in \mathbb{Z} \mid 1 = 4u + 7v$. Aplicando el algoritmo extendido de Euclídes, llegamos a que $1 = 4 \cdot 2 + 7(-1)$. Luego:

$$4 \cdot 2 \equiv 1 \mod (7) \Longrightarrow 4 \cdot 2 \cdot 6 \equiv 6 \mod (7) \Longrightarrow 4 \cdot 12 \equiv 6 \mod (7)$$

Por lo que $x_0 = 12$ es solución particular del sistema.

No obstante, no es la óptima, ya que $12 \neq 0$ y $|12| \not< |7|$. Dividimos $x_0 = 12$ entre 7 para buscar la óptima: $12 = 7 \cdot 1 + 5 \Longrightarrow y_0 = 5$ es la solución óptima.

Por tanto, la ecuación es equivalente a $x \equiv 5 \mod (7)$ y sus soluciones son: $\{5 + 7k \mid k \in A\}$.

2. $1100x \equiv 660 \mod (140)$.

$$1100x \equiv 660 \mod (140) \overset{8)}{\iff} 110x \equiv 66 \mod (14) \overset{8)}{\iff} 55x \equiv 33 \mod (7)$$

$$\left.\begin{array}{l} 55x \equiv 33 \mod (7) \\ 55 = 11 \cdot 5 \\ 33 = 11 \cdot 3 \\ \mcd(11,7) = 1 \end{array}\right\} \overset{7)}{\iff} 5x \equiv 3 \mod (7)$$

$$\left.\begin{array}{l} 5x \equiv 3 \mod (7) \\ 5x \equiv -2x \mod (7) \\ 3 \equiv -4 \mod (7) \end{array}\right\} \overset{1)}{\iff} -2x \equiv -4 \mod (7)$$

$$\left.\begin{array}{l} -2x \equiv -4 \mod (7) \\ -2 = -2 \cdot 1 \\ -4 = -2 \cdot 2 \\ \mcd(-2,7) = 1 \end{array}\right\} \overset{7)}{\iff} x \equiv 2 \mod (7)$$

$|2| < |7| \implies y_0 = 2$ es solución óptima del sistema. Por tanto, el conjunto de soluciones de la ecuación es:

$$\{2 + 7k \mid k \in A\}$$

Una solución alternativa al ejercicio es, cuando tenemos $5x \equiv 3 \mod (7)$, podemos darnos cuenta de que $5^{-1} = 3$ en $\mathbb{Z}_7$.

$$5x \equiv 3 \mod (7) \Leftrightarrow 5 \cdot 5^{-1}x \equiv 3 \cdot 3 \mod (7) \Leftrightarrow x \equiv 2 \mod (7)$$

3.7.2. Sistemas de 2 ecuaciones de congruencias

Sea A un DE, queremos resolver sistemas de ecuaciones de congruencias con dos ecuaciones de la forma:

$$\left.\begin{array}{ll} a_1x \equiv b_1 & \mod (m_1) \\ a_2x \equiv b_2 & \mod (m_2) \end{array}\right\}$$

Con $a_i, b_i, m_i \in A \mid a_i \neq 0 \neq m_i$ con $i \in \{1, 2\}$.

Supongamos que cada ecuación tiene solución (de forma independiente) y entonces $\exists a, b \in A$ tales que el sistema anterior es equivalente a uno de la forma:

$$\left.\begin{array}{ll} x \equiv a & \mod (m) \\ x \equiv b & \mod (n) \end{array}\right\}$$

Con $a, b, m, n \in A \mid m \neq 0 \neq n$.

Teorema 3.32. *Sea A un DE y consideramos un sistema de la forma:*

$$\left.\begin{array}{ll} x \equiv a & \mod (m) \\ x \equiv b & \mod (n) \end{array}\right\}$$

Con $a, b, m, n \in A \mid m \neq 0 \neq n$.

Sean $d = \mcd(m, n)$, $p = \mcm(m, n)$:

i) El sistema tiene solución $\iff a \equiv b \mod (d)$.

ii) Si el sistema tiene solución. Entonces, existe una solución:

$$x_0 \in A \mid x_0 = 0 \ \vee \ \phi(x_0) < \phi(p)$$

Que llamaremos ***solución óptima del sistema****. Por tanto, el resto de soluciones serán de la forma:*

$$\{x_0 + kp \mid k \in A\}$$

Y por tanto, el sistema será equivalente a la ecuación:

$$x \equiv x_0 \mod (p)$$

Demostración. Suponemos inicialmente que la primera ecuación tiene solución, ya que si no la tuviera, tenemos claro que el sistema tampoco.

i) La solución general de la primera ecuación es, por el Teorema 3.31:

$$x = a + km \mid k \in A$$

Sustituimos en la segunda ecuación y, entonces, el sistema tiene solución si la ecuación

$$a + km \equiv b \mod (n)$$

Con incógnita k tiene solución:

$$a+km \equiv b \mod (n) \iff km \equiv b-a \mod (n) \iff d|b-a \iff a \equiv b \mod (d)$$

ii) Suponemos que tiene solución $\implies km \equiv b - a \mod (m)$.
Sea k_0 una solución particular, sabemos que la solución general es:

$$k = k_0 + t\frac{m}{d} \ \ \forall t \in A$$

$$x = a + km \implies x = a + \left(k_0 + t\frac{m}{d}\right) n = a + k_0 n + t\frac{mn}{d} = a + k_0 n + tp$$

Por lo que $x_0 = a + k_0 n$ es una solución particular del sistema y las demás son:

$$\{x_0 + tp \mid t \in A\}$$

Si dividimos x_0 entre p, obtenemos que $x_0 = qp + y_0$ con $y_0 = 0 \vee \phi(y_0) < \phi(p)$.

$$y_0 \equiv x_0 \mod (p)$$

Luego y_0 también es solución del sistema; es la óptima.

□

Ejemplo. Calcular la menor capacidad posible de un depósito sabiendo que a un depóstio de doble capacidad le ha faltado 1 litro para llenarlo con garrafas de 5 litros y que a uno de quíntuple capacidad le ha faltado también 1 litro para llenarlo con garrafas de 7 litros.

Sea x la capacidad buscada:

$$2x+1 \text{ es divisible por } 5 \text{ y } 5x+1 \text{ es divisible por } 7 \text{ luego:}$$

$$\left.\begin{array}{lll} 2x+1 \equiv 0 & \text{mód } (5) & \iff 2x \equiv -1 \quad \text{mód } (5) \\ 5x+1 \equiv 0 & \text{mód } (7) & \iff 5x \equiv -1 \quad \text{mód } (7) \end{array}\right\}$$

Buscamos la solución de cada sistema (si una no tiene solución, el sistema no tiene solución):

$$\left.\begin{array}{l} 2x \equiv -1 \quad \text{mód } (5) \\ -1 \equiv 4 \quad \text{mód } (5) \end{array}\right\} \iff 2x \equiv 4 \quad \text{mód } (5)$$

$$\left.\begin{array}{l} 2x \equiv 4 \quad \text{mód } (5) \\ \text{mcd}(2,5) = 1 \end{array}\right\} \iff x \equiv 2 \quad \text{mód } (5)$$

$$\left.\begin{array}{l} 5x \equiv -1 \quad \text{mód } (7) \\ -1 \equiv 6 \quad \text{mód } (7) \end{array}\right\} \iff 5x \equiv 6 \quad \text{mód } (7)$$

$$\text{mcd}(5,7) = 1 \ \wedge \ 1|6 \implies \text{tiene solución.}$$

Buscamos la solución de la segunda ecuación, buscando la identidad de Bezout para 5 y 7:

$$1 = 5 \cdot 3 + 7(-2) \implies 5 \cdot 3 \equiv 1 \quad \text{mód } (7) \iff 5 \cdot 3 \cdot 6 \equiv 6 \quad \text{mód } (7)$$

Por lo que $x_0 = 3 \cdot 6 = 18$ es una solución particular.
Recordamos que en $\mathbb{Z}$, la función euclídea es el valor absoluto, antes de continuar.
$|18| \not< |7|$. $18 = 2 \cdot 7 + 4 \implies y_0 = 4$ es la solución óptima de la ecuación.
Por tanto, la ecuación es equivalente a: $x \equiv 4 \ \text{mód } (7)$ y el sistema es equivalente a:

$$\left.\begin{array}{ll} x \equiv 2 & \text{mód } (5) \\ x \equiv 4 & \text{mód } (7) \end{array}\right\}$$

Que tiene solución si:
$2 \equiv 4 \ \text{mód } (\text{mcd}(5,7)) \iff 2 \equiv 4 \ \text{mód } (1) \iff 2 - 4 \in 1A = A$, Cierto.

La solución de la primera ecuación es $x = 2 + 5k \mid k \in A$. Sustituimos en la segunda:

$$2 + 5k \equiv 4 \quad \text{mód } (7) \iff 5k \equiv 2 \quad \text{mód } (7)$$

Buscamos la identidad de Bezout:

$$1 = 5 \cdot 3 + 7(-2) \implies 5 \cdot 3 \equiv 1 \quad \text{mód } (7) \iff 5 \cdot 3 \cdot 2 \equiv 2 \quad \text{mód } (7)$$

Luego $k_0 = 6$ es solución particular de esta. De hecho es la óptima, ya que $|6| < |7|$.
La solucón general es $k = 6 + 7t \mid t \in A$.

Entonces:

$$x = 2 + 5k = 2 + 5(6 + 7t) = 32 + 35t \mid t \in \mathbb{Z}$$

Siendo 32 la solución óptima del sistema.

Buscamos la menor solución no negativa del sistema, que resulta ser la óptima. Por tanto, el depósito era de 32 litros.

3.7.3. Sistemas de r ecuaciones de congruencias

Sea $r \geqslant 2$, consideramos un sistema de la forma:

$$\left.\begin{array}{ll} a_1x \equiv b_1 & \text{mód } (m_1) \\ a_2x \equiv b_2 & \text{mód } (m_2) \\ & \vdots \\ a_rx \equiv b_r & \text{mód } (m_r) \end{array}\right\}$$

1. Resolvemos cada una de forma independiente y si todas tienen solución, el sistema será equivalente a:

$$\left.\begin{array}{ll} x \equiv c_1 & \text{mód } (n_1) \\ x \equiv c_2 & \text{mód } (n_2) \\ & \vdots \\ x \equiv c_r & \text{mód } (n_r) \end{array}\right\}$$

Para ciertos $c_1, c_2, \ldots, c_r, n_1, n_2, \ldots, n_r \in A$.
2. Resolvemos el sistema de las dos primeras ecuaciones y si tiene solución, obtendremos una ecuación $x \equiv c \mod (n)$ con $n = \text{mcm}(n_1, n_2), c \in A$ equivalente a dicho sistema:

$$\left.\begin{array}{ll} x \equiv c & \text{mód } (n) \\ x \equiv c_2 & \text{mód } (n_2) \\ & \vdots \\ x \equiv c_r & \text{mód } (n_r) \end{array}\right\}$$

3. Repetimos el proceso $r - 1$ veces, obteniendo que si todos los sistemas anteriores tenían solución, el sistema de r ecuaciones es equivalente a una ecuación del tipo:

$$x \equiv a \mod (m)$$

Para cierto $a \in A$ y $m = \text{mcm}(n_1, n_2, \ldots, n_r)$, que tendrá como solución el conjunto:

$$\{a + km \mid k \in A\}$$

3.8. Anillos cocientes

Sea A un anillo conmutativo e $I \subseteq A$ un ideal.
Sabemos que $\equiv \mod (I)$ es una relación de equivalencia. Consideramos el conjunto cociente:

$$A/(\equiv \mod (I)) =: A/I = \{[a] \mid a \in A\}$$

$$[a] = \{b \in A \mid b \equiv a \mod (I)\} = \{b \in A \mid b - a \in I\} = \{a + y \mid y \in I\}$$

Notaremos a la clase de cada elemento $a \in A$ por $a + I$:

$$[a] =: a + I$$

A la que llamaremos **clase de** a **módulo** I. Por tanto:

$$A/I = \{a + I \mid a \in A\}$$

Notemos que:

$$a + I = b + I \iff a \equiv b \mod (I)$$

Definimos en A/I las operaciones suma y producto $\forall a_1 + I, a_2 + I$ de la forma:

$$(a_1 + I) + (a_2 + I) := (a_1 + a_2) + I$$

$$(a_1 + I)(a_2 + I) := (a_1 a_2) + I$$

Demostración.
Veamos que se encuentran bien definidas (que no dependen del representante):

$$\text{Suponemos} \quad \left.\begin{array}{rcl} a_1 + I = b_1 + I & \Longrightarrow & a_1 \equiv b_1 \mod (I) \\ a_2 + I = b_2 + I & \Longrightarrow & a_2 \equiv b_2 \mod (I) \end{array}\right\} \Longrightarrow$$

$$\Longrightarrow \left\{\begin{array}{c} a_1 + a_2 \equiv b_1 + b_2 \mod (I) \\ a_1 a_2 \equiv b_1 b_2 \mod (I) \end{array}\right\} \Longrightarrow \left\{\begin{array}{c} (a_1 + a_2) + I = (b_1 + b_2) + I \\ (a_1 a_2) + I = (b_1 b_2) + I \end{array}\right.$$

□

Proposición 3.33. *Se verifica que con estas operaciones, A/I es un anillo conmutativo, que llamaremos* ***anillo cociente de*** A ***sobre el ideal*** I *ó* ***anillo de restos módulo*** I*.*

Demostración.

$$\forall a + I, b + I, c + I \in A/I$$

Asociativa de la suma:

$$((a + I) + (b + I)) + (c + I) = ((a + b) + I) + (c + I) = (a + b + c) + I =$$

$$= (a + I) + ((b + c) + I) = (a + I) + ((b + I) + (c + I))$$

Conmutativa de la suma:

$$(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I)$$

Existencia de elemento neutro de la suma:

$$0 + I \in A/I \mid (a + I) + (0 + I) = (a + 0) + I = a + I$$

Existencia de opuestos:

$$(-a) + I \in A/I \mid ((-a) + I) + (a + I) = (-a + a) + I = 0 + I$$

Asociativa del producto:

$$((a+I)(b+I))(c+I) = ((ab)+I)(c+I) = (abc)+I = (a+I)((bc)+I) = (a+I)((b+I)(c+I))$$

Conmutativa del producto:

$$(a + I)(b + I) = (ab) + I = (ba) + I = (b + I)(a + I)$$

Existencia de elemento neutro del producto:

$$1 + I \in A/I \mid (a + I)(1 + I) = (a \cdot 1) + I = a + I$$

Propiedad distributiva:

$$(a + I)((b + I) + (c + I)) = (a + I)((b + c) + I) = (a(b + c)) + I =$$

$$= (ab + ac)I = ((ab) + I) + ((ac) + I) = (a + I)(b + I) + (a + I)(c + I)$$

Por lo que A/I es un anillo conmutativo. □

Notemos que si $A = \mathbb{Z}$ e $I = n\mathbb{Z}$.
Entonces, como $a \equiv b \mod (n) \iff aR_nb \ \ \forall a, b \in \mathbb{Z}$:

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/R_n = \mathbb{Z}_n$$

Definición 3.15 (Núcleo de homomorfismo)**.** Sea $f : A \to B$ un homomorfismo de anillos, definimos su **núcleo**, notado $Ker(f)$, como:

$$Ker(f) = \{a \in A \mid f(a) = 0\}$$

Proposición 3.34. *Sea A un anillo conmutativo y consideramos un homomorfismo $f : A \Longrightarrow B$ de anillos. Entonces:*

$$Ker(f) \text{ es un ideal de } A$$

Demostración.

$$\forall a, b \in Ker(f) \Longrightarrow f(a + b) = f(a) + f(b) = 0 + 0 = 0 \Longrightarrow a + b \in Ker(f)$$

$$\forall a \in Ker(f) \ \ \forall c \in A \Longrightarrow f(ca) = f(c)f(a) = f(c) \cdot 0 = 0 \Longrightarrow ca \in Ker(f)$$

□

Antes de ver el siguiente teorema, recordamos la Proposición **??**.

Teorema 3.35 (Primer teorema de isomorfía)**.**
Todo homomorfismo de anillos conmutativos $f : A \to B$ induce un isomorfismo

$$\overline{f} : A/Ker(f) \Longrightarrow Img(f)$$

Definido por:

$$\overline{f}(a + Ker(f)) := f(a) \qquad \forall a + Ker(f) \in A/Ker(f)$$

Demostración.
1) Veamos que $\overline{f}$ está bien definida y que no depende de representantes:

$$\text{Sea } a + Ker(f) = b + Ker(f) \Longleftrightarrow a \equiv b \mod (Ker(f)) \Longleftrightarrow a - b \in Ker(f)$$

$$0 = f(a - b) = f(a) - f(b) \Longleftrightarrow f(a) = f(b)$$

2) Ahora, veamos que $\overline{f}$ es un homomorfismo. $\forall a, b \in A/Ker(f)$:

$$\overline{f}((a + Ker(f)) + (b + Ker(f))) = \overline{f}((a + b) + Ker(f)) = f(a + b) = f(a) + f(b)$$

$$\overline{f}((a + Ker(f))(b + Ker(f))) = \overline{f}((ab) + Ker(f)) = f(ab) = f(a)f(b)$$

$$\overline{f}(1 + Ker(f)) = f(1) = 1$$

3) Veamos que $\overline{f}$ es sobreyectiva:

$$Img(\overline{f}) = \{\overline{f}(a) \mid a \in A/Ker(f)\} = \{f(a) \mid a \in A\} = Img(f)$$

4) Veamos que $\overline{f}$ es inyectiva:

$$\forall a + Ker(f), b + Ker(f) \in A/Ker(f) \mid \overline{f}(a + Ker(f)) = \overline{f}(b + Ker(f))$$

$$\overline{f}(a + Ker(f)) = \overline{f}(b + Ker(f)) \Longrightarrow f(a) = f(b) \Longrightarrow 0 = f(a) - f(b) = f(a - b)$$

$$f(a-b) = 0 \Longrightarrow a-b \in Ker(f) \Longrightarrow a \equiv b \mod (Ker(f)) \Longrightarrow a+Ker(f) = b+Ker(f)$$

□

Teorema 3.36. *Sea A un DE y $I = mA$ con $m \in A \mid m \neq 0 \ \wedge \ m \notin \mathcal{U}(A)$. Entonces:*

i) $a + mA \in \mathcal{U}(A/mA) \Longleftrightarrow \text{mcd}(a, m) = 1$.

ii) Los siguientes enunciados son equivalentes:

1) m es irreducible.

2) A/mA es un cuerpo.

3) A/mA es un DI.

Demostración.
i)
$\Longrightarrow$) Sea $a + mA \in \mathcal{U}(A/mA)$. Entonces:

$$\exists b + mA \in A/mA \mid 1 + mA = (a + mA)(b + mA) = (ab) + mA \Longrightarrow$$

$$\Longrightarrow ab \equiv 1 \mod (m) \Longrightarrow m|ab - 1 \Longrightarrow \exists q \in A \mid ab - 1 = qm$$

$$\left.\begin{array}{r} 1 = ab - qm \\ d = \mathrm{mcd}(a, b) \end{array}\right\} \Longrightarrow d|1 \Longrightarrow d \in \mathcal{U}(A) \Longrightarrow d \sim 1 \Longrightarrow \mathrm{mcd}(a, m) = \mathrm{mcd}(a, 1) = 1$$

$\Longleftarrow$) Sea $\mathrm{mcd}(a, m) = 1$, elegimos los coeficientes de Bezout:

$$u, v \in A \mid 1 = au + mv \Longrightarrow au \equiv 1 \mod (m) \Longrightarrow$$

$$\Longrightarrow (a + mA)(u + mA) = (au) + mA = 1 + mA \Longrightarrow a + mA \in \mathcal{U}(A/mA)$$

ii)
1) $\Longrightarrow$ 2) Suponemos que m es irreducible:

$$\forall a + mA \in A/mA \mid a + mA \neq 0 + mA \Longrightarrow a \notin mA \Longrightarrow m \not| a$$

Como m es irreducible y $m \not| a \Longrightarrow \mathrm{mcd}(a, m) = 1$.
Por i), tenemos que $a + mA \in \mathcal{U}(A/mA) \Longrightarrow \mathcal{U}(A/mA) = A/mA \setminus \{0\} \Longrightarrow A/mA$ es un cuerpo.
2) $\Longrightarrow$ 3) Cierto por el Lema **??**.
3) $\Longrightarrow$ 1) Suponemos que A/mA es DI $\Longrightarrow m \neq 0 \ \wedge \ m \notin \mathcal{U}(A)$

$$\forall a \in A \mid a|m \Longrightarrow \exists b \in A \mid m = ab \Longrightarrow$$

$$\Longrightarrow 0 + mA = m + mA = (ab) + mA = (a + mA)(b + mA)$$

Como A es DI:

$$a + mA = 0 + mA \Longrightarrow a \in mA \Longrightarrow a = ma' \quad a' \in A$$

$$m = ab \Longrightarrow m = ma'b \Longrightarrow a'b = 1 \Longrightarrow b \in \mathcal{U}(A) \Longrightarrow a \sim m \Longrightarrow m \text{ irreducible}$$

ó

$$b + mA = 0 + mA \Longrightarrow b \in mA \Longrightarrow b = mb' \quad b' \in A$$

$$m = ab \Longrightarrow m = mab' \Longrightarrow ab' = 1 \Longrightarrow a \in \mathcal{U}(A) \Longrightarrow b \sim m \Longrightarrow m \text{ irreducible}$$

□

Ejemplo. Sea $A = \mathbb{Z}$, consideramos $I = 153\mathbb{Z}$ y $\mathbb{Z}/153\mathbb{Z} = \mathbb{Z}_{153}$.
Estudiar si $2 \in \mathcal{U}(\mathbb{Z}_{153})$ y encontrar 2^{-1}.

$$\mathrm{mcd}(2, 153) = 1 \Longrightarrow 2 \in \mathcal{U}(\mathbb{Z}_{153})$$

Buscamos los coeficientes de Bezout: $1 = 2(-76) + 153 \cdot 1$:

$$2(-76) \equiv 1 \mod (153) \Longrightarrow 2^{-1} = -76 = 153 - 76 = 77$$

Corolario 3.36.1. *del Teorema 3.36.*
1) Sea $n \geqslant 2$. Entonces $\mathbb{Z}_n$ es un cuerpo $\iff$ n es irreducible (primo en $\mathbb{Z}$).
2) Sea K un cuerpo y $f \in K[x] \mid f \neq 0 \ \wedge \ f \notin \mathcal{U}(K[x])$ es decir, f no es constante. Entonces:

$$K[x]/fK[x] \text{ es un cuerpo } \iff f \text{ es irreducible}$$

3) Sea $n \in \{-2,-1,2,3\}$ y $\alpha \in \mathbb{Z}[\sqrt{n}] \mid \alpha \neq 0 \ \wedge \ \alpha \notin \mathcal{U}(\mathbb{Z}[\sqrt{n}])$ es decir, $N(\alpha) \notin \{0,-1,1\}$. Entonces:

$$\mathbb{Z}[\sqrt{n}]/\alpha\mathbb{Z}[\sqrt{n}] \text{ es un cuerpo } \iff \alpha \text{ es irreducible.}$$

Por tanto, sabemos que si $p \in \mathbb{Z}$ es primo $\implies \mathbb{Z}_p$ es un cuerpo finito de p elementos:

$$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$$

Proposición 3.37. *Sea $p \in \mathbb{Z}$ irreducible (primo), consideramos $\mathbb{Z}_p[x]$ y $f \in \mathbb{Z}_p[x] \mid f = a_0 + a_1x + \ldots + a_nx^n \ n \geqslant 1$. Entonces:*

$$\mathbb{Z}_p[x]/f\mathbb{Z}_p[x] \text{ es finito}$$

Demostración.
$\forall g + f\mathbb{Z}_p[x] \in \mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$ dividimos g entre f:

$$g = fq + r \mid r = 0 \ \vee \ grd(r) < grd(f) = n$$

$$r = b_0 + b_1x + \ldots + b_{n-1}x^{n-1} \quad b_i \in \mathbb{Z}_p \ \forall i \in \{1, \ldots, n\}$$

Luego $g - r = fq \implies g \equiv r \mod (f) \implies g + f\mathbb{Z}_p[x] = r + f\mathbb{Z}_p[x]$
Por lo que todos los elementos de $\mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$ son de la forma:

$$c_0 + c_1x + \ldots + c_{n-1}x^{n-1} \quad \forall c_i \in \mathbb{Z}_p \ \forall i \in \{1, \ldots, n\}$$

Es decir, en $\mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$ hay p^n elementos. □

Teorema 3.38 (Teorema de Moore)**.** *Sea $p \in \mathbb{Z}$ irreducible y $f \in \mathbb{Z}_p[x]$ irreducible. Entonces:*

$$\mathbb{Z}_p[x]/f\mathbb{Z}_p[x] \text{ es un cuerpo con } p^n \text{ elementos.}$$

$$\mathbb{Z}_p[x]/f\mathbb{Z}_p[x] =: \mathbb{F}p^n$$

Demostración. Véase el Teorema 3.36 y la Proposición 3.37. □

Definición 3.16 (Primos relativos)**.** Sea A un DI, dos elementos $a, b \in A$ diremos que son **primos relativos** si:

$$\text{mcd}(a, b) = 1$$

Definición 3.17 (Función de Euler)**. La función de Euler** es una aplicación:

$$\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$$

Definida por:

$$\varphi(n) = |\{m \in \mathbb{N} \mid 1 \leqslant m \leqslant n \ \wedge \ \text{mcd}(m, n) = 1\}|$$

Es decir, la función de Euler cuenta el número de primos relativos que son menores a un cierto n:

$$\varphi(1) = 1$$
$$\varphi(2) = 1$$
$$\varphi(3) = 2$$
$$\varphi(4) = 2$$
$$\varphi(5) = 4$$

Notemos que:

$$\varphi(n) = |\mathcal{U}(\mathbb{Z}_n)|$$

Ya que:

$$\mathcal{U}(\mathbb{Z}_n) = \{m \in \mathbb{Z}_n \mid \text{mcd}(m, n) = 1\}$$

Proposición 3.39. *Sean A y B dos anillos conmutativos. Entonces:*

$$A \times B$$

Es un anillo conmutativo.

Demostración. Buscamos definir unas aplicaciones suma y producto que cumplan con las condiciones para que $A \times B$ sea un anillo conmutativo.
Definimos $+ : A \times B \to A \times B$ como:

$$(a, b) + (c, d) := (a + c, b + d) \qquad \forall (a, b), (c, d) \in A \times B$$

Y definimos también $\cdot : A \times B \to A \times B$ como:

$$(a, b) \cdot (c, d) := (ac, bd) \qquad \forall (a, b), (c, d) \in A \times B$$

Veamos que con esta suma y producto $A \times B$ es un anillo conmutativo: $\forall (a, b), (c, d), (e, f) \in A \times B$:

Asociativa de la suma:

$$((a, b) + (c, d)) + (e, f) = (a + c, b + d) + (e, f) = (a + c + e, b + d + f) =$$

$$= (a, b) + (c + e, d + f) = (a, b) + ((c, d) + (e, f))$$

Conmutativa de la suma:

$$(a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b)$$

Existencia de elemento neutro de la suma:

$$(0, 0) \in A \times B \mid (0, 0) + (a, b) = (a + 0, b + 0) = (a, b)$$

Existencia de opuesto:

$$(-a,-b) \in A \times B \mid (-a,-b) + (a+b) = (-a+a, -b+b) = (0,0)$$

Asociativa del producto:

$$((a,b)(c,d))(e,f) = (ac,bd)(e,f) = (ace,bdf) =$$

$$= (a,b)(ce,df) = (a,b)((c,d)(e,f))$$

Conmutativa del producto:

$$(a,b)(c,d) = (ac,bd) = (ca,db) = (c,d)(a,b)$$

Existencia de elemento netro del producto:

$$(1,1) \in A \times B \mid (1,1)(a,b) = (a \cdot 1, b \cdot 1) = (a,b)$$

Propiedad distributiva:

$$(a,b)((c,d)+(e,f)) = (a,b)(c+e,d+f) = (a(c+e), b(d+f)) =$$

$$= (ac+ae, bd+bf) = (ac,bd) + (ae,bf) = ((a,b)(c,d)) + ((a,b)(e,f))$$

□

Notemos que si tenemos A, B anillos conmutativos y consideramos $A \times B$, este último conjunto puede ser también un anillo conmutativo con suma y producto distintas a las especificadas en la proposición.

Teorema 3.40 (Teorema chino del resto)**.**
Sea A un DE y $m, n \in A \mid \text{mcd}(m,n) = 1$. Entonces:

$$A/(mn)A \cong A/mA \times A/nA$$

Demostración. Definimos la aplicación $f : A \to A/mA \times A/nA$ por:

$$f(a) = (a+mA, a+nA) \quad \forall a \in A$$

Que es un homomorfismo de anillos. $\forall a, b \in A$:

$$f(a+b) = ((a+b)+mA, (a+b)+nA) = ((a+mA)+(b+mA), (a+nA)+(b+nA)) =$$

$$= (a+mA, a+nA) + (b+mA, b+nA) = f(a) + f(b)$$

$$f(ab) = ((ab)+mA, (ab)+nA) = ((a+mA)(b+mA), (a+nA)(b+nA)) =$$

$$= (a+mA, a+nA)(b+mA, b+nA) = f(a)f(b)$$

$$f(1) = (1+mA, 1+nA)$$

Veamos además que f es un epimorfismo (que es sobreyectiva):
Sea $(a+mA, b+nA) \in A/mA \times A/nA$, consideramos el sistema:

$$\begin{cases} x \equiv a \mod (m) \\ x \equiv b \mod (n) \end{cases}$$

Que tiene solución, ya que $a \equiv b \mod (\mathrm{mcd}(n,m)) \iff a \equiv b \mod (1)$, cierto $\forall a, b \in A$

Luego $\exists x_0 \in A$ tal que:

$$\left.\begin{array}{rcl} x_0 \equiv a \mod (m) & \iff & x_0 + mA = a + mA \\ x_0 \equiv b \mod (n) & \iff & x_0 + nA = b + nA \end{array}\right\} \Longrightarrow f(x_0) = (a + mA, b + nA)$$

Aplicando el Primer Teorema de Isomorfía, tenemos que f induce un isomorfismo:

$$\overline{f} : A/Ker(f) \to Img(f) = A/mA \times A/nA$$

$$\overline{f}(a + Ker(f)A) := f(a) = (a + mA, a + nA) \quad \forall a + Ker(f)A \in A/Ker(f)$$

Veamos que $Ker(f) = (mn)A$:

$$Ker(f) = \{a \in A \mid f(a) = (0{+}mA, 0{+}nA)\} = \{a \in A \mid a{+}mA = 0{+}mA \wedge a{+}nA = 0{+}nA\} =$$

$$= \{a \in A \mid a \equiv 0 \mod (m) \ \wedge \ a \equiv 0 \mod (n)\} = \{a \in A \mid m|a \ \wedge \ n|a\}$$

Si $a \in Ker(f) \Longrightarrow m|a \ \wedge \ n|a \Longrightarrow \mathrm{mcm}(m,n)|a$.

$$\left.\begin{array}{l} \mathrm{mcm}(m,n)|a \\ \mathrm{mcd}(m,n) = 1 \end{array}\right\} \Longrightarrow \mathrm{mcm}(m,n) = mn \Longrightarrow mn|a \Longrightarrow a \in (mn)A$$

Luego $Ker(f) \subseteq (mn)A$.

Si $a \in (mn)A \Longrightarrow f(a) = (a + mA, a + nA)$. Pero:
$a \in (mn)A \Longrightarrow a \in mA \Longrightarrow a + mA = 0 + mA$
$a \in (mn)A \Longrightarrow a \in nA \Longrightarrow a + nA = 0 + nA$
Luego $a \in Ker(f) \Longrightarrow (mn)A \subseteq Ker(f)$

Y por doble inclusión tenemos que $Ker(f) = (mn)A$.

Por lo que tenemos un isomorfismo:

$$\overline{f} : A/(mn)A \to A/mA \times A/nA$$

Por lo que $A/(mn)A \cong A/mA \times A/nA$ □

Corolario 3.40.1. *de 3.40.*
Sean $m,\ n \in \mathbb{Z} \mid m, n \geqslant 2$ *y* $\mathrm{mcd}(m,n) = 1$. *Entonces:*

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

Notemos que si $f : A \to B$ es un isomorfismo de anillos, la restricción de f a $\mathcal{U}(A)$ nos da una biyección

$$f : \mathcal{U}(A) \to \mathcal{U}(B)$$

Ya que si f es un homomorfismo y $a \in \mathcal{U}(A) \Longrightarrow f(a) \in \mathcal{U}(B)$.
Por tanto, $|\mathcal{U}(A)| = |\mathcal{U}(B)|$.

Aunque no nos será necesario ahora, damos la definición de número primo:

Definición 3.18 (Primo)**.** Sea A un DI. Un elemento $p \in A$ diremos que es primo si $p \neq 0$, $p \notin \mathcal{U}(A)$ y siempre que:

$$p|ab \Longrightarrow p|a \ \wedge \ p|b \qquad \forall a, b \in A$$

Considerando el contrarrecíproco, que si $a, b \in A \mid p \not| a \ \wedge \ p \not| b \Longrightarrow p \not| ab$

Lema 3.41. *Sea p primo, $p \geqslant 2$, $m \in \mathbb{N}$ con $m \geqslant 1$ y $e \in \mathbb{N} \mid e \geqslant 1$. Entonces:*

$$\text{mcd}(m, p^e) = 1 \Longleftrightarrow p \not| m$$

Proposición 3.42. *Sea φ la función de Euler. Se verifica:*
1) Sean $m, n \in \mathbb{N} \mid m, n \geqslant 2 \ \wedge \ \text{mcd}(m, n) = 1 \Longrightarrow \varphi(mn) = \varphi(m)\varphi(n)$.
2) Sea p primo con $p \geqslant 2$ y $e \in \mathbb{N} \mid e \geqslant 1 \Longrightarrow \varphi(p^e) = p^{e-1}(p-1)$.
3) Sea $n \in \mathbb{N}$ con $n \geqslant 2$ y $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ su factorización en primos:

$$\varphi(n) = p_1^{e_1-1} p_2^{e_2-1} \dots p_r^{e_r-1}(p_1 - 1)(p_2 - 1) \dots (p_r - 1)$$

Demostración.
1)

$$\varphi(mn) = |\mathcal{U}(\mathbb{Z}_{mn})|$$

Como $\text{mcd}(m, n) = 1$, aplicando el Teorema Chino del Resto:

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

y dicho isomorfismo induce una biyección:

$$\mathcal{U}(\mathbb{Z}_{mn}) \cong \mathcal{U}(\mathbb{Z}_m \times \mathbb{Z}_n)$$

$$\varphi(mn) = |\mathcal{U}(\mathbb{Z}_{mn})| = |\mathcal{U}(\mathbb{Z}_m \times Z_n)| = |\mathcal{U}(\mathbb{Z}_m) \times \mathcal{U}(\mathbb{Z}_n)| = |\mathcal{U}(\mathbb{Z}_m)||\mathcal{U}(\mathbb{Z}_n)| = \varphi(m)\varphi(n)$$

2)

$$\varphi(p^e) = |\{m \in \mathbb{N} \mid 1 \leqslant m \leqslant p^e \ \wedge \ \text{mcd}(m, p^e) = 1\}| =$$
$$= p^e - |\{m \in \mathbb{Z} \mid 1 \leqslant m \leqslant p^e \ \wedge \ \text{mcd}(m, p^e) \neq 1\}|$$

Por el Lema 3.41 tenemos que $\text{mcd}(m, p^e) = 1 \Longleftrightarrow p \not| m$. Luego:

$$\text{mcd}(m, p^e) \neq 1 \Longleftrightarrow p|m$$
$$\varphi(p^e) = p^e - |\{m \in \mathbb{N} \mid 1 \leqslant m \leqslant p^e \ \wedge \ p|m\}| =$$
$$= p^e - |\{pk \mid 1 \leqslant k \leqslant p^{e-1}\}| = p^e - p^{e-1} = p^{e-1}(p-1)$$

3)

$$\varphi(n) = \varphi(p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}) \overset{1)}{=} \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \dots \varphi(p_r^{e_r}) \overset{2)}{=}$$
$$= p_1^{e_1-1}(p_1 - 1) p_2^{e_2-1}(p_2 - 1) \dots p_r^{e_r-1}(p_r - 1) =$$
$$= p_1^{e_1-1} p_2^{e_2-1} \dots p_r^{e_r-1}(p_1 - 1)(p_2 - 1) \dots (p_r - 1)$$

□

Proposición 3.43. *Sea A un anillo conmutativo con $|\mathcal{U}(A)| = r \geqslant 1$ y sea $u \in \mathcal{U}(A)$. Se verifica que:*

$$u^r = 1$$

Demostración. Sea $\mathcal{U}(A) = \{u_1, u_2, \ldots, u_r\}$. Tomamos $u \in \mathcal{U}(A)$.
Definimos $f : \mathcal{U}(A) \to \mathcal{U}(A)$ por:

$$f(u_i) := uu_i \qquad \forall u_i \in \mathcal{U}(A)$$

Veamos que f es inyectiva. Sean $u_i, u_j \in \mathcal{U}(A) \mid f(u_i) = f(u_j)$:

$$f(u_i) = f(u_j) \Longrightarrow uu_i = uu_j \Longrightarrow u_i = u^{-1}uu_j = u_j$$

Como $\mathcal{U}(A)$ es finito $\Longrightarrow$ f es biyectiva $\Longrightarrow$ es sobreyectiva $\Longrightarrow$ $Img(f) = \mathcal{U}(A)$

$$Img(f) = \{f(u_i) \mid u_i \in \mathcal{U}(A)\} = \{uu_1, uu_2, \ldots, uu_r\} = \mathcal{U}(A) = \{u_1, u_2, \ldots, u_r\}$$

Luego:

$$\prod_{i=1}^{r} uu_i = \prod_{i=1}^{r} u_i \Longrightarrow u^r \prod_{i=1}^{r} u_i = \prod_{i=1}^{r} u_i \Longrightarrow u^r = 1$$

□

Teorema 3.44 (de Euler)**.** *Sea $n \in \mathbb{Z} \mid n \geqslant 2$. $\forall a \in \mathbb{Z} \mid \text{mcd}(a, b) = 1$. Se verifica:*

$$a^{\varphi(n)} \equiv 1 \mod (n)$$

Demostración.
Sea $a \in \mathbb{Z}$ con $n \in \mathbb{Z} \mid n \geqslant 2 \mid \text{mcd}(a, n) = 1$. Entonces, por el Teorema 3.36:

$$\text{mcd}(a, n) = 1 \Longrightarrow a + n\mathbb{Z} \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$$

Como $\varphi(n) = |\mathcal{U}(\mathbb{Z}/n\mathbb{Z})|$, por la Proposición 3.43:

$$\left.\begin{array}{l}(a + n\mathbb{Z})^{\varphi(n)} = 1 + n\mathbb{Z} \\ (a + n\mathbb{Z})^{\varphi(n)} = a^{\varphi(n)} + n\mathbb{Z}\end{array}\right\} \Longrightarrow a^{\varphi(n)} \equiv 1 \mod (n)$$

□

Teorema 3.45 (El pequeño Teorema de Fermat)**.**
Sea $p \in \mathbb{Z}$, $p \geqslant 2$ primo. $\forall a \in \mathbb{Z} \mid p \nmid a$. Se verifica que:

$$a^{p-1} \equiv 1 \mod (p) \Longleftrightarrow a^p \equiv a \mod (p)$$

Demostración. Sea $p \in \mathbb{Z} \mid p \geqslant 2$ primo $a \in \mathbb{Z} \mid p \nmid a$. Por el Lema 3.41:

$$p \nmid a \Longrightarrow \text{mcd}(a, p) = 1$$

Luego por el Teorema 3.44:

$$\left.\begin{array}{l}a^{\varphi(p)} \equiv 1 \mod (p) \\ \varphi(p) = p - 1\end{array}\right\} \Longrightarrow a^{p-1} \equiv 1 \mod (p) \Longleftrightarrow a^p \equiv a \mod (p)$$

□

Corolario 3.45.1. *del Teorema 3.44.*
Sea $n \geqslant 2$. Entonces $\forall r \in \mathcal{U}(\mathbb{Z}_n)$, se verifica que:

$$r^{\varphi(n)} = 1 \text{ en } \mathbb{Z}_n \iff r^{-1} = r^{\varphi(n)-1}$$

Demostración. Por el Teorema 3.44, tenemos que:

$$r^{\varphi(n)} \equiv 1 \mod (n) \iff r^{\varphi(n)} = 1 \text{ en } \mathbb{Z}_n \iff r^{-1} = r^{\varphi(n)-1}$$

Donde el último paso se obtiene muliplicando por r^{-1} en ambos lados. □

Corolario 3.45.2. *del Teorema 3.45.*
Sea $p \in \mathbb{Z}$, $p \geqslant 2$ primo. Entonces $\forall r \in \mathbb{Z}_p$, $r \neq 0$. Se verifica que:

$$r^{p-1} = 1 \text{ en } \mathbb{Z}_p \iff r^p = r \text{ en } \mathbb{Z}_p$$

Demostración.

$$\mathbb{Z}_p = \{0, 1, \ldots, p-1\} \implies \forall r \in \mathbb{Z}_p \mid r \neq 0 \implies p \not| r$$

Aplicando el Teorema 3.45, tenemos que:

$$r^{p-1} \equiv 1 \mod (p) \iff r^{p-1} = 1 \text{ en } \mathbb{Z}_p \iff r^p = r \text{ en } \mathbb{Z}_p$$

Donde el último paso se obtiene muliplicando por r en ambos lados. □

Ejemplo. Calcular el resto de dividir 279^{323} entre 17.

Calculamos el resto de dividir 279 entre 17: Como $279 = 17 \cdot 16 + 7$:

$$279 \equiv 7 \mod (17) \implies 279^{323} \equiv 7^{323} \mod (17)$$

Por tanto, el resto buscado es el mismo resto que al dividir 7^{323} entre 17.

Como $\text{mcd}(7, 17) = 1 \implies 7^{\varphi(17)} \equiv 1 \mod (17)$, por el Teorema 3.44.
Como 17 es primo: $\varphi(17) = 17 - 1 = 16$, por la Proposición 3.42. Por lo que:

$$7^{16} \equiv 1 \mod (17)$$

Dividimos 323 entre 16:

$$323 = 20 \cdot 16 + 3$$

$$7^{323} = 7^{16 \cdot 20 + 3} = (7^{16})^{20} \cdot 7^3 \equiv 1 \cdot 7^3 = 7^3 \mod (17)$$

Donde hemos aplicado que:

$$7^{16} \equiv 1 \mod (17) \implies (7^{16})^{20} \equiv 1^{20} \mod (17)$$

Finalmente, calculamos el resto de dividir 7^3 entre 17: $7^3 = 343 = 20 \cdot 17 + 3 \implies 7^3 \equiv 3 \mod (17)$. Luego:

$$279^{323} \equiv 3 \mod (17)$$

Por lo que:

$$R(279^{323}; 17) = 3$$

Teorema 3.46 (Teorema chino del resto generalizado)**.**
Sea A un DE y $m_1, m_2, \ldots, m_k \in A$ con $k \geqslant 2$ tales que $\mathrm{mcd}(m_i, m_j) = 1$ $\forall i, j \in \{1, \ldots, k\} \mid i \neq j$. *Entonces:*

$$A/(m_1 m_2 \ldots m_k)A \cong A/m_1 A \times A/m_2 A \times \ldots \times A/m_k A$$

Lema 3.47.
Sea A un DE y $m_1, m_2, \ldots, m_k \in A$ con $k \geqslant 2$ tales que $\mathrm{mcd}(m_i, m_j) = 1$ $\forall i, j \in \{1, \ldots, k\} \mid i \neq j$. *Entonces, $\forall a_1, a_2, \ldots, a_k \in A$, el sistema:*

$$\begin{cases} x \equiv a_1 \mod (m_1) \\ x \equiv a_2 \mod (m_2) \\ \vdots \\ x \equiv a_k \mod (m_k) \end{cases}$$

Tiene solución.

Además, si $c \in A$ es una solución particular del sistema, entonces sl sistema es equivalente a:

$$x \equiv c \mod (m_1 m_2 \ldots m_k)$$

Demostración. Realizamos inducción en k.
Si $k = 2$, tenemos un sistema de la forma:

$$\begin{cases} x \equiv a_1 \mod (m_1) \\ x \equiv a_2 \mod (m_2) \end{cases}$$

Que tiene solución $\iff a_1 \equiv a_2 \mod (\mathrm{mcd}(m_1, m_2)) \iff a_1 \equiv a_2 \mod (1)$, cierto siempre.
Además, si c es una solución particular $\implies$ sabemos que el sistema es equivalente a:

$$x \equiv c \mod (\mathrm{mcm}(m_1, m_2))$$

Pero como $\mathrm{mcd}(m_1, m_2) = 1 \implies \mathrm{mcm}(m_1, m_2) = m_1 m_2$. Luego el sistema es equivlente a:

$$x \equiv c \mod (m_1 m_2)$$

Sea $k > 2$ y supongamos que:

$$\begin{cases} x \equiv a_1 \mod (m_1) \\ x \equiv a_2 \mod (m_2) \\ \vdots \\ x \equiv a_{k-1} \mod (m_{k-1}) \end{cases}$$

Tiene solución y que si $d \in A$ es una solución particular, entonces el sistema es equivalente a:

$$x \equiv d \mod (m_1 m_2 \ldots m_{k-1})$$

Consideramos el sistema:

$$\begin{cases} x \equiv a_1 \mod (m_1) \\ x \equiv a_2 \mod (m_2) \\ \vdots \\ x \equiv a_k \mod (m_k) \end{cases}$$

Que es equivalente a:

$$\begin{cases} x \equiv d \mod (m_1 m_2 \dots m_{k-1}) \\ x \equiv a_k \mod (m_k) \end{cases}$$

Puesto que $\text{mcd}(m_k, m_i) = 1 \ \ \forall i \in \{1, \dots, k-1\}$.
Entonces: $\text{mcd}(m_1 m_2 \dots m_{k-1}, m_k) = 1$. Luego:

$d \equiv a_k \mod (\text{mcd}(m_1 m_2 \dots m_{k-1}, m_k)) \iff d \equiv a_k \mod (1) \iff$ el sistema tiene solución

Además, como $\text{mcd}(m_1 m_2 \dots m_{k-1}, m_k) = 1 \implies \text{mcm}(m_1 m_2 \dots m_{k-1}, m_k) = m_1 m_2 \dots m_{k-1} m_k$.

Por lo que el sistema será equivalente a (si c es una solución particular):

$$x \equiv c \mod (m_1 m_2 \dots m_k)$$

□

4. Dominios de factorización única

Definición 4.1 (Divisor propio)**.** Sea A un DI y $a \in A$. Un divisor no trivial de a será un **divisor propio de** a. Es decir, es

$$b \in A \mid b \notin U(A) \ \wedge \ b|a \ \wedge \ a \not| b$$

Definición 4.2 (Dominio de Factoriazación Única)**.**
Sea A un DI. Diremos que es un **dominio de factorización única** (abreviado DFU), si $\forall a \in A \mid a \neq 0 \ \wedge \ a \notin U(A)$ podemos expresarlo como:

$$a = p_1 p_2 \dots p_s \mid p_i \text{ es irreducible } \ \forall i \in \{1, \dots, s\}$$

Además, tal factorización es esencialmente única en el sentido de que si:

$$a = q_1 q_2 \dots q_r \mid q_i \text{ es irreducible } \ \forall i \in \{1, \dots, r\}$$

Es otra factorización en irreducibles de a, entonces tenemos que $r = s$ y que, reordenando si fuera necesario:

$$p_i \sim q_i \ \ \forall i \in \{1, \dots, s\}$$

Ejemplo. Un ejemplo de que dos factorizaciones sean esencialmente iguales es, por ejemplo:

$$-6 = -2 \cdot 3$$

$$-6 = 2 \cdot (-3)$$

$$2 \sim -2 \ \wedge \ 3 \sim -3$$

En cualquier dominio de integridad A, podemos elegir un conjunto $P \neq 0$ representativo de sus elementos irreducibles, en el siguiente sentido:

1) $\forall p \in P \Rightarrow p$ es irreducible.

2) Si $q \in A$ irreducible $\Rightarrow \exists p \in P \mid p \sim q$.

3) Si $p, p' \in P \mid p \neq p' \Rightarrow p \not\sim p'$.

Ejemplo. Ejemplos del conjunto P son:

$$\text{En } \mathbb{Z} \quad P = \{p \in \mathbb{Z} \mid p \text{ es irreducible} \quad \wedge \quad p > 0\}$$

$$\text{En } K[x] \quad P \text{ es el conjunto de polinomios irreducibles mónicos}$$

Notemos que si A es un DFU, todo elemento $a \in A \mid a \neq 0$ se expresa de forma esencialmente única como:

$$a = up_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

Donde $u \in U(A)$, $r \geqslant 0$
$p_i \in P \ \forall i \in \{1, \dots, r\}, p_i \neq p_j \ \forall i, j \in \{1, \dots, r\} \quad i \neq j$
$e_i \in \mathbb{Z} \mid e_i \geqslant 1$

Notación. $\forall a \in A$, $a \neq 0$ y $\forall p \in P$, denotaremos por:

$$e(p, a)$$

Al exponente del irreducible p en la factorización de a, entendiendo que si p no aparece en la factorización de a, entonces $e(p, a) = 0$. Por tanto, sea A un DFU, notaremos $\forall a \in A$:

$$a = u \prod_{p \in P} p^{e(p,a)} \qquad u \in U(A)$$

Lema 4.1. *Sea A un DFU con $a, b \in A$ tales que $a \neq 0 \neq b$ y $p \in P$:*

$$e(p, ab) = e(p, a) + e(p, b)$$

Lema 4.2. *Sea A un DFU con $a, b, c \in A$ tales que $a, b, c \neq 0$:*

$$a|c \Leftrightarrow e(p, a) \leqslant e(p, c) \quad \forall p \in P$$

Proposición 4.3. *Sea A un DFU y $a, b \in A$ tales que:*

$$a = u \prod_{p \in P} p^{e(p,a)} \qquad b = v \prod_{p \in P} p^{e(p,b)} \quad u, v \in U(A)$$

Entonces, $\exists mcd(a, b) \ \wedge \ mcm(a, b)$ tales que:

$$mcd(a, b) = \prod_{p \in P} p^{\text{mín}\{e(p,a), e(p,b)\}}$$

$$mcm(a, b) = \prod_{p \in P} p^{\text{máx}\{e(p,a), e(p,b)\}}$$

Recordamos ahora la definición de número primo, Definición 3.18.

Proposición 4.4. *Sea A un DI:*

1) $\forall p \in A$ primo $\Rightarrow p$ es irreducible.

2) Si A es además un DFU y $p \in A$ irreducible $\Rightarrow p$ es primo.

Demostración.
1) Sea $p \in A$ primo.
Supongamos que $a \in A \mid a|p \Rightarrow \exists b \in A \mid p = ab \Rightarrow p|ab \Rightarrow p|a \ \vee \ p|b$.
Si $p|a \Rightarrow p \sim a$.
Si $p|b \Rightarrow \exists c \in A \mid b = pc = abc \Rightarrow 1 = ac \Rightarrow a \in U(A)$.
Por lo que los únicos divisores de p son los triviales $\Rightarrow p$ es irreducible.

2) Sea A un DFU y $p \in A \mid p$ irreducible (Luego $p \neq 0 \ \wedge \ p \notin U(A)$).
Sean $a, b \in A \mid p|ab \Rightarrow e(p,p) = 1 \leqslant e(p,ab) = e(p,a) + e(p,b)$. Entonces:

$$\left.\begin{array}{lcl} e(p,a) \geqslant 1 & \Rightarrow & p|a \\ \vee & & \\ e(p,b) \geqslant 1 & \Rightarrow & p|b \end{array}\right\} \Rightarrow p \text{ primo}$$

□

Corolario 4.4.1. *de la Proposición 4.4.*
Sea A un DFU y $p \in A$:

$$p \text{ es primo } \Leftrightarrow p \text{ es irreducible}$$

Teorema 4.5 (Caracterización de los DFUs)**.**
Sea A un DI, son equivalentes:
i) A es un DFU.
ii) Se verifica en A:

$$\forall a \in A \mid a \neq 0 \ \wedge \ a \notin U(A) \text{ se expresa como producto de irreducibles}$$

$$\exists mcd(a,b) \ \wedge \ \exists mcm(a,b) \ \ \forall a, b \in A$$

iii) Se verifica en A:

$$\forall a \in A \mid a \neq 0 \ \wedge \ a \notin U(A) \text{ se expresa como producto de irreducibles}$$

$$\forall p \in A \text{ irreducible } \Rightarrow p \text{ primo}$$

Lema 4.6. *Sea A un DE con función euclídea ϕ, $a, b \in A$ tal que a es un divisor propio de b. Entonces:*

$$\phi(a) < \phi(b)$$

Teorema 4.7. *Sea A un DE $\Rightarrow$ A es un DFU.*

Demostración. Sea A un DE con función euclídea ϕ:
Sabemos que por ser A DE $\Rightarrow \exists mcd(a,b) \ \wedge \ \exists mcm(a,b) \ \ \forall a, b \in A$.
Veamos que $\forall a \in A \mid a \neq 0 \ \wedge \ a \notin U(A)$ podemos expresar a como producto de irreducibles, por lo que según el Teorema 4.5, A sería un DFU:

Supongamos que no: $\exists a \in A \mid a \neq 0 \ \wedge \ a \notin U(A)$ que no puede expresarse como producto de irreducibles, por lo que sabemos que no es irreducible $\Rightarrow \exists a_1 \in A \mid a_1$ es divisor propio de a.
Por tanto, $\exists b_1 \in A \mid a = a_1 b_1$ y $a_1 \ \vee \ b_1$ no puede expresarse como producto de

irreducibles.

Supongamos (lo que no nos hace perder generalidad) que es a_1 el que no puede expresarse como producto de irreducibles. Por lo que a_1 no es irreducible y sbemos que $\exists a_2 \in A$ divisor propio de a_1 que no puede expresarse como producto de irreducibles.

COntinuando con este razonamiento, llegamos a una sucesión no finita :

$$a_0 = a, a_1, a_2, \ldots, a_n, \ldots \mid a_i \text{ es divisor propio de } a_{i-1} \quad \forall i \geqslant 1$$

Siendo ninguno de ellos producto de irreducibles y:

$$\phi(a_0) > \phi(a_1) > \phi(a_2) > \ldots > \phi(a_n) > \ldots$$

Una sucesión estrictamente decreciente de números naturales. Contradicción, luego $\forall a \in A$, a puede expresarse como producto de irreducibles, haciendo que A sea un DFU. □

Corolario 4.7.1 (Teorema fundamental de la aritmética)**.** *El anillo $\mathbb{Z}$ es un DFU.*

Demostración. Por la Proposición **??**, sabemos que $\mathbb{Z}$ es un DE y ahora, por el Teorema 4.7, sabemos que $\mathbb{Z}$ es un DFU. □

Corolario 4.7.2. *Sea K un cuerpo. Entonces $K[x]$ es un DFU.*

Demostración. Por el Teorema **??**, sabemos que $K[x]$ es un DE y ahora, por el Teorema 4.7, sabemos que $K[x]$ es un DFU. □

Corolario 4.7.3. *Sea $n \in \{-2, -1, 2, 3\}$. Entonces $\mathbb{Z}[\sqrt{n}]$ es un DFU.*

Demostración. Por el Teorema **??**, sabemos que $\mathbb{Z}[\sqrt{n}]$ es un DU y ahora, por el Teorema 4.7, sabemos que $\mathbb{Z}[\sqrt{n}]$ es un DFU. □

Veremos también que hay anillos que son DFU y no son DE:

Proposición 4.8. *$\mathbb{Z}[x]$ no es DE.*

Demostración.
Para ello, podemos ver que $\exists I \subseteq \mathbb{Z}[x]$ ideal $\mid I \neq m\mathbb{Z}[x] \quad \forall m \in \mathbb{Z}[x]$:
Sea $I = \left\{ p = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x] \mid a_0 \in 2\mathbb{Z} \right\}$ es un ideal de $\mathbb{Z}[x]$:

$$\forall f = \sum_{i=0}^{n} a_i x^i, \ g = \sum_{j=0}^{m} b_j x^j \in I \Rightarrow a_0, b_0 \in 2\mathbb{Z}$$

$$s = f + g = \sum_{i=0}^{\text{máx}\{n,m\}} (a_i + b_i) x^i \Rightarrow s_0 = a_0 + b_0 \in 2\mathbb{Z} \Rightarrow s \in I$$

$$p = fg = \sum_{k=0}^{n+m} k_i x^i \mid k_i = \sum_{i+j=k} a_i b_j \Rightarrow k_0 = a_0 b_0 \in 2\mathbb{Z} \Rightarrow p \in I$$

Veamos ahora que I no es principal. Si lo fuera, $\exists f \in \mathbb{Z}[x] \mid I = f\mathbb{Z}[x]$:

$$2 \in I = f\mathbb{Z}[x] \Rightarrow \exists g \in \mathbb{Z}[x] \mid fg = 2$$

$$0 = grd(2) = grd(fg) = grd(f) + grd(g) \Rightarrow grd(f) = 0 = grd(g)$$

Luego $f = a \ \wedge \ g = b$ con $a, b \in \mathbb{Z}$ y:

$$2 = ab \Rightarrow \begin{cases} a = \pm 2 & \wedge & b = \pm 1 \\ \vee & & \\ a = \pm 1 & \wedge & b = \pm 2 \end{cases}$$

$$I = f\mathbb{Z}[x] = a\mathbb{Z}[x]$$

$$\text{Si } a = \pm 2 \Rightarrow x \notin I \ \underline{\text{Contradicción}}$$

$$\text{Si } a = \pm 1 \Rightarrow I = \pm\mathbb{Z}[x] = \mathbb{Z}[x] \Rightarrow 1 \in I \ \underline{\text{Contradicción}}$$

Luego $\nexists f \in \mathbb{Z}[x] \mid I = f\mathbb{Z}[x] \Rightarrow I$ no es principal $\Rightarrow \mathbb{Z}[x]$ no es DE. □

Veremos más tarde (en el Teorema 4.17) que $\mathbb{Z}[x]$ es un DFU.

4.1. Irreducibles y primos en el anillo de enteros cuadráticos

Lema 4.9. *Sean $\alpha, \beta \in \mathbb{Z}[\sqrt{n}]$ tales que α es divisor propio de β en $\mathbb{Z}[\sqrt{n}]$. Entonces:*

$$N(\alpha) \text{ es divisor propio de } N(\beta) \text{ en } \mathbb{Z}$$

Demostración. Sea α divisor propio de β:
Sabemos por tanto que $\alpha \notin U(\mathbb{Z}[\sqrt{n}]) \Rightarrow N(\alpha) \neq \pm 1 \Rightarrow N(\alpha) \notin U(\mathbb{Z})$.

$$\exists \gamma \in \mathbb{Z}[\sqrt{n}] \mid \gamma \notin U(\mathbb{Z}[\sqrt{n}]) \ \wedge \ \beta = \alpha \cdot \gamma \Rightarrow N(\beta) = N(\alpha \cdot \gamma) = N(\alpha)N(\gamma)$$

Como $\alpha \notin U(\mathbb{Z}[\sqrt{n}]) \Rightarrow N(\alpha) \notin U(\mathbb{Z})$.
Luego $N(\alpha) | N(\beta)$ y es un divisor propio suyo. □

Teorema 4.10. *En $\mathbb{Z}$ hay infinitos números primos.*

Demostración. Supongamos que en $\mathbb{Z}$ hay n primos positivos: $\{p_1, p_2, \ldots, p_n\}$.
Sea $a = p_1 p_2 \ldots p_n + 1 \Rightarrow a \in \mathbb{Z} \wedge \mathbb{Z}$ es DFU $\Rightarrow a$ tiene factorización en irreducibles:

$$\exists i \in \{1, \ldots, n\} \mid p_i | a = p_1 p_2 \ldots p_n + 1 \Rightarrow p_i | 1 \Rightarrow p_i \in U(\mathbb{Z}) \Rightarrow p_i = \pm 1$$

Contradicción con que era irreducible. Luego en $\mathbb{Z}$ hay una cantidad no numerable de números primos. □

Proposición 4.11. *Sea $n \in \mathbb{Z} \mid \sqrt{n} \notin \mathbb{Z}$ y $\alpha \in \mathbb{Z}[\sqrt{n}]$. Entonces:*
1) Si $N(\alpha) = \pm p$ primo de $\mathbb{Z} \Rightarrow p$ es irreducible.
2) Si α es primo $\Rightarrow N(\alpha) \in \{\pm p, \pm p^2\}$ con $p \in \mathbb{Z}$ primo.
Si $N(\alpha) = \pm p^2 \Rightarrow \alpha \sim p$, son asociados en $\mathbb{Z}[\sqrt{n}]$.

Demostración.

2) α primo $\Rightarrow \alpha \neq 0 \ \wedge \ \alpha \notin U(\mathbb{Z}[\sqrt{n}]) \Rightarrow N(\alpha) \notin \{0, \pm 1\}$.

$$\left.\begin{array}{l} N(\alpha) = \alpha \cdot \overline{\alpha} \in \mathbb{Z} \\ \mathbb{Z} \text{ es un DFU} \end{array}\right\} \Rightarrow \alpha \cdot \overline{\alpha} = p_1 \ldots p_k \mid p_i \in P \ \ \forall i \in \{1, \ldots, k\}$$

En $\mathbb{Z}[\sqrt{n}]$:

$$\alpha | \alpha \cdot \overline{\alpha} \Rightarrow \alpha | p_1 \ldots p_k$$

α es primo $\Rightarrow \exists i \in \{1, \ldots, k\} \mid \alpha | p_i$. Sea $p = p_i$:

Hemos encontrado un primo $p \in \mathbb{Z}$ tal que $\alpha | p$ en $\mathbb{Z}[\sqrt{n}] \Rightarrow \exists \beta \in \mathbb{Z}[\sqrt{n}] \mid p = \alpha\beta$.

$$N(p) = p^2 = N(\alpha \cdot \beta) = N(\alpha)N(\beta) \Rightarrow N(\alpha) | p^2 \wedge N(\alpha) \neq \pm 1 \Rightarrow N(\alpha) \in \{\pm p, \pm p^2\}$$

Supongamos que $N(\alpha) = \pm p^2$:

$$p^2 = N(\alpha)N(\beta) = \pm p^2 N(\beta) \Rightarrow N(\beta) = \pm 1 \Rightarrow \beta \in U(\mathbb{Z}[\sqrt{n}]) \Rightarrow$$

$$\Rightarrow p = \alpha \cdot \beta \text{ es asociado a } \alpha$$

□

Lema 4.12. *Sea $\alpha = a + bi \in \mathbb{Z}[i] \mid a, b \neq 0$. Entonces:*

$$\alpha \text{ es primo o irreducible } \Leftrightarrow N(\alpha) \text{ es un número primo en } \mathbb{Z}$$

Notemos que puede haber irreducibles cuya norma no sea un número primo o su opuesto: En $\mathbb{Z}[\sqrt{-5}]$, $\alpha = 3$ es irreducible (visto en el Ejemplo **??**). Sin embargo, $N(3) = 9$, que no es primo en $\mathbb{Z}$. Además, notemos que:

$$\text{Si } N(\alpha) = p^2 \not\Rightarrow \alpha \text{ es irreducible}$$

En $Z[i]$, sea $\alpha = 2$, $N(\alpha) = 4 = 2^2$

$$2 = (1+i)(1-i) \Rightarrow \text{ no es irreducible}$$

Ejemplo.
1. Factorizar $\alpha = 11 + 7i$ en $\mathbb{Z}[i]$.

(Como $\mathbb{Z}[i]$ es DFU, podemos usar que $p \in \mathbb{Z}[i]$ es primo $\Leftrightarrow p$ es irreducible).

$$N(\alpha) = 11^2 + 7^2 = 170 = 2 \cdot 5 \cdot 17$$

$N(\alpha)$ no es primo ni cuadrado de primo $\Rightarrow \alpha$ no es irreducible.
Como ningún cuadrado de primo divide a $N(\alpha)$, buscamos elementos en $\mathbb{Z}[i]$ de norma 2, 5 ó 17 que dividan a α:

$$a + bi \in \mathbb{Z}[i] \mid N(a+bi) = a^2 + b^2 = 2 \Leftrightarrow \begin{cases} a = \pm 1 \\ b = \pm 1 \end{cases}$$

Los elementos de norma 1 son $1 + i$ y sus asociados.

$$\frac{11+7i}{1+i} = \frac{(11+7i)(1-i)}{2} = \frac{11 - 11i + 7i + 7}{2} = \frac{18 - 8i}{2} = 9 - 2i$$

Luego $\alpha = (1+i)(9-2i)$ con $1+i$ irreducible por ser $N(1+i) = 2$, primo en $\mathbb{Z}$.

$N(9-2i) = 5 \cdot 17$, buscamos elementos de norma 5:

$$a + bi \in \mathbb{Z}[i] \mid N(a+bi) = a^2 + b^2 = 5 \Leftrightarrow \begin{cases} a = \pm 2 & \wedge & b = \pm 1 \\ \vee & & \\ a = \pm 1 & \wedge & b = \pm 2 \end{cases}$$

Los elementos de norma 5 son $2 + i$, $1 + 2i$ y sus asociados.

$$\frac{9-2i}{2+i} = \frac{(9-2i)(2-i)}{5} = \frac{18 - 9i - 4i - 2}{5} = \frac{16}{5} - \frac{13}{5}i$$

Luego $2 + i \not| 9 - 2i$ en $\mathbb{Z}[i]$.

$$\frac{9-2i}{1+2i} = \frac{(9-2i)(1-2i)}{5} = \frac{5 - 20i}{5} = 1 - 4i$$

Luego $9 - 2i = (1+2i)(1-4i)$ con $1+2i$, $1-4i$ irreducibles por ser $N(1+2i) = 5$, $N(1-4i) = 17$, primos.

En definitiva, $\alpha = 11 + 7i = (1+i)(1+2i)(1-4i)$

2) Sea $\beta = 2i \in \mathbb{Z}[i]$, calcular $mcd(\alpha, \beta), mcm(\alpha, \beta)$:

$$\beta = 2i = (1+i)(1-i)i = (1+i)^2$$

$$mcd(\alpha, \beta) = 1 + i$$

$$mcm(\alpha, \beta) = (1+i)^2(1+2i)(1-4i) = 18 - 4i$$

Donde hemos aplicado la Proposición 4.3.

Ejemplo. Existen elementos irreducibles que no son primos:
Sea $\mathbb{Z}[\sqrt{-5}]$, consideramos $\alpha = 1 + \sqrt{-5}$, $\alpha \neq 0 \ \wedge \ \alpha \notin U(\mathbb{Z}[\sqrt{-5}])$. Veamos que α es irreducible:
Sea $\beta \in \mathbb{Z}[\sqrt{-5}] \mid \beta | \alpha \Rightarrow N(\beta) | N(\alpha) = 6 = 2 \cdot 3$. Las opciones son:

$$\begin{cases} N(\beta) = 1 & \Rightarrow \beta \in U(\mathbb{Z}[\sqrt{-5}]) \\ N(\beta) = 2 & \exists a, b \in \mathbb{Z} \mid a^2 + 5b^2 = 2 \\ N(\beta) = 3 & \exists a, b \in \mathbb{Z} \mid a^2 + 5b^2 = 3 \end{cases}$$

Luego $\beta \in U(\mathbb{Z}[\sqrt{-5}]) \Rightarrow \alpha$ es irreducible.

Veamos que α no es primo:

$$\left.\begin{array}{rcl} N(\alpha) = 6 = \alpha \cdot \overline{\alpha} & \Rightarrow & \alpha | 6 = 2 \cdot 3 \\ \left.\begin{array}{l} N(\alpha) \not| N(2) \\ N(\alpha) \not| N(3) \end{array}\right\} & \Rightarrow & \alpha \not| 2 \ \wedge \ \alpha \not| 3 \end{array}\right\} \Rightarrow \alpha \text{ no es primo}$$

4.2. Factoriazación en el anillo de polinomios

Sabemos que si K es un cuerpo $\Rightarrow K[x]$ es un DE $\Rightarrow K[x]$ es un DFU.
Nuestro primer objetivo será demostrar que si A es un DFU $\Rightarrow A[x]$ es un DFU.

Sea A un DFU y $K = \mathbb{Q}(A)$, vamos a intentar relacionar a los irreducibles de $A[x]$ con los de $K[x]$.

Proposición 4.13. *Sea $a \in A$. Entonces:*

$$a \text{ es irreducible en } A \Leftrightarrow a \text{ es irreducible en } A[x]$$

Notemos que en $K[x]$ no hay irreducibles de grado 0, puesto que serían unidades.

Demostración.
$\Longrightarrow$) Sea $a \in A$ irreducible en A, luego $a \neq 0 \ \wedge \ a \notin U(A) = U(A[x])$.
Si $f \in A[x]$ es un divisor de a:

$$\exists g \in A[x] \mid a = fg \Rightarrow 0 = grd(a) = grd(fg) = grd(f) + grd(g)$$

$grd(f) = 0 \Rightarrow f \in A \Rightarrow f \in U(A) = U(A[x])$ ó f asociado a a en A
Por lo que a es también un irreducible en $A[x]$.

$\Longleftarrow$) Supongamos que a es irreducible en $A[x]$ y que no lo es en A:
Luego $\exists b \in A$ divisor propio de $a \Rightarrow b \in A[x]$ divisor propio de a.
Contradicción, luego a es irreducible en A. □

Definición 4.3 (Contenido de un polinomios)**.**
Sea A un DFU y sea $f = \sum_{i=0}^{n} a_i x^i \in A[x]$ con $n \geqslant 1$. Definimos el **contenido de** f, notado $C(f)$ como:

$$C(f) := mcd(a_0, a_1, \ldots, a_n)$$

Si $C(f) = 1$, diremos que f es un **polinomio mónico**.

Lema 4.14. *Sea A un DFU y $K = \mathbb{Q}(A)$. Se verifica:*
i) $\forall a \in A \ \wedge \ \forall f \in A[x]$ con $grd(f) \geqslant 1 \Rightarrow C(af) = aC(f)$.
ii) $\forall f \in A[x] \mid grd(f) \geqslant 1$ se expresa de forma única como $f = af'$ tal que:

$$a = C(f) \ \wedge \ f' \in A[x] \mid f' \text{ es primitivo}$$

iii) $\forall \phi \in K[x] \mid grd(\phi) \geqslant 1$ se expresa de forma única como $\phi = \frac{a}{b} f$ tal que:

$$\frac{a}{b} \in K \ \wedge \ f \in A[x] \mid f \text{ es primitivo}$$

Demostración.
i) Sea $f = \sum_{i=0}^{n} a_i x^i$ con $n \geqslant 1 \Rightarrow af = \sum_{i=0}^{n} aa_i x^i$.

$$C(af) = mcd(aa_0, aa_1, \ldots, aa_n) = mcd(a_0, a_1, \ldots, a_n)a = aC(f)$$

ii) Sea $f = \sum_{i=0}^{n} a_i x^i$ con $n \geqslant 1$. Sea $a = C(f) = mcd(a_0, a_1, \ldots, a_n)$
Consideramos $a'_i = \frac{a_i}{a} \quad \forall i \in \{1, \ldots, n\}$
Sea $f' = \sum_{i=0}^{n} a'_i x^i$. Se verifica que $af' = f$ y que:

$$C(f) = mcd(a'_0, a'_1, \ldots, a'_n) = 1$$

Luego f' es primitivo.

Falta ver la unicidad de f' y a:
Sea $f = bg'$ con $b \in A$ y $g' \in A[x]$ primitivo:

$$C(f) = C(bg') = bC(g') = b \Rightarrow a = b$$

$$f = af' = ag' \overset{DI}{\Rightarrow} f' = g'$$

iii) Sea $\phi = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i \in K[x]$ con $n \geqslant 1$. Sea $b = b_1 b_2 \ldots b_n \in A$

$$b\phi = \sum_{i=0}^{n} b\frac{a_i}{b_i} x^i \qquad c_i = b\frac{a_i}{b_i} \in A \quad \forall i \in \{1, \ldots, n\} \Rightarrow b\phi \in A[x]$$

Ya que $c_i = a_i b_1 \ldots b_{i-1} b_{i+1} \ldots b_n$

Aplicando ii):

$$b\phi = af \mid a = C(b\phi) \ \wedge \ f \in A[x] \text{ primitivo}$$

Por lo que tenemos que:

$$\phi = \frac{a}{b} f = \frac{a}{b_1 b_2 \ldots b_n} f$$

Falta ver la unicidad de $\frac{a}{b} \in K$ y de $f \in A[x]$:
Sea $\phi = \frac{a'}{b'} f' \mid f'$ primitivo:

$$\frac{a}{b} f = \frac{a'}{b'} f' \Rightarrow b'af = ba'f'$$

$$C(b'af) = C(ba'f') \Rightarrow b'aC(f) = ba'C(f') \Rightarrow b'a = ba' \Rightarrow \frac{a}{b} = \frac{a'}{b'}$$

Y tenemos que:

$$\phi = \frac{a}{b} f = \frac{a}{b} f' \overset{DI}{\Rightarrow} f = f'$$

□

Lema 4.15 (de Gauss)**.** *El producto de polinomios primitivos es primitivo.*

Corolario 4.15.1. *del Lema 4.15.*
Sean $f, g \in A[x] \mid grd(f), grd(g) \geqslant 1$. *Entonces:*

$$C(fg) = C(f)C(g)$$

Demostración. Tenemos por el Lema 4.14 que:

$$f = C(f)f' \quad g = C(g)g' \mid f', g' \text{ primitivos} \Rightarrow f'g' \text{ primitivo}$$

$$fg = C(f)C(g)f'g' \Rightarrow C(fg) = C(f)C(g)C(f'g') = C(f)C(g)$$

□

Teorema 4.16. *Sea* A *un DFU y* $K = \mathbb{Q}(A)$. *Sea* $\phi \in K[x]$ *con* $grd(\phi) \geqslant 1$ *y sea* $\phi = \frac{a}{b}f \mid f \in A[x]$ *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.
ϕ y f son asociados en $K[x] \Rightarrow Div(\phi) = Div(f) \Rightarrow (i) \Leftrightarrow ii))$

2) $\Rightarrow$ 3) Supongamos que f no es irreducible en $A[x]$:
$\exists f_1$ divisor propio de $f \Rightarrow \exists f_2 \in A[x] \mid f = f_1 f_2$.
• Si f_1 es constante $\Rightarrow f_1 \in A \Rightarrow C(f) = 1 = f_1 C(f_2) \Rightarrow$
$\Rightarrow f_1 \in U(A) = U(A[x]) \Rightarrow f_1$ no es divisor propio. Contradicción.
• Si f_2 es constante $\Rightarrow f_2 \in A \Rightarrow C(f) = 1 = f_2 C(f_1) \Rightarrow$
$\Rightarrow f_2 \in U(A) = U(A[x]) \Rightarrow f_1$ no es divisor propio. Contradicción.
• Si f_1 y f_2 no son constantes:

$$grad(f_1), grd(f_2) \geqslant 1$$

Entonces: $f = f_1 f_2$ es factorización en polinomios no unidades en $K[x]$. Contradicción.
Luego f es irreducible en $A[x]$.

3) $\Rightarrow$ 2) Supongamos que $f = \phi_1\phi_2 \in K[x]$ con $grd(\phi_1), grd(\phi_2) \geqslant 1$.

$$\phi_1 = \frac{a_1}{b_1}f_1 \quad \phi_2 = \frac{a_2}{b_2}f_2 \mid f_1, f_2 \in A[x] \text{ primitivos}$$

$$f = \frac{a_1a_2}{b_1b_2}f_1f_2 \Rightarrow b_1b_2f = a_1a_2f_1f_2 \Rightarrow C(b_1b_2f) = C(a_1a_2f_1f_2)$$

$$C(b_1b_2f) = b_1b_2C(f) = b_1b_2$$

$$C(a_1a_2f_1f_2) = a_1a_2C(f_1f_2) = a_1a_2C(f_1)C(f_2) = a_1a_2$$

$$b_1b_2 = a_1a_2 \Rightarrow \frac{a_1a_2}{b_1b_2} = 1 \Rightarrow f = f_1f_2 \text{ Contradicción}$$

Ya que f era irreducible en $A[x]$.
Por tanto, f es irreducible en $K[x]$. □

Corolario 4.16.1. *del Teorema 4.16.*
Sea A DFU, $f \in A[x] \mid grd(f) \geqslant 1$. Entonces:

$$f \text{ es irreducible en } A[x] \Leftrightarrow f \text{ es primitivo e irreducible en } K[x]$$

Teorema 4.17 (de Gauss)**.** *Si A es DFU $\Rightarrow A[x]$ es DFU.*

Demostración.
Sea $f \in A[x]$, $f \neq 0 \ \wedge \ f \notin U(A[x])$. Veamos que se expresa como producto de irreducibles.

• Si $grd(f) = 0 \Rightarrow f \in A \Rightarrow f = p_1 \dots p_k$ con $p_i \in A$ irreducible
$\forall i \in \{1, \dots, k\} \Rightarrow p_i \in A[x] \Rightarrow f$ admite factorización en irreducibles en $A[x]$.
• Si $grd(f) \geq 1 \Rightarrow f = af' \mid f \in A[x]$ primitivo.

$$\left.\begin{array}{l} f' \in K[x] = \mathbb{Q}(A) \\ K[x]DFU \end{array}\right\} \Rightarrow f' = \phi_1 \dots \phi_s$$

Con $\phi_i \in K[x]$ irreducible $\forall i \in \{1, \dots, s\}$

$a \in A \Rightarrow a$ admite factorización en irreducibles: $a = p_1 \dots p_k$.

$$\phi_i = \frac{a_i}{b_i} f_i \mid f_i \in A[x] \text{ primitivo e irreducible } \forall i \in \{1, \dots, s\}$$

Luego:

$$f' = \frac{a_1 \dots a_s}{b_1 \dots b_s} f_1 \dots f_s$$

$$1 = C(f') = C\left(\frac{a_1 \dots a_s}{b_1 \dots b_s} f_1 \dots f_s\right) = \frac{a_1 \dots a_s}{b_1 \dots b_s} C(f_1 \dots f_s) =$$
$$= \frac{a_1 \dots a_s}{b_1 \dots b_s} C(f_1) \dots C(f_s) = \frac{a_1 \dots a_s}{b_1 \dots b_s}$$

Luego:

$$f = af' = p_1 \dots p_k f_1 \dots f_s$$

Es una factorización en irreducibles.

Veamos ahora que todo irreducible de $A[x]$ es primo, para así tener que $A[x]$ es un DFU mediante el Teorema 4.5.

Sea $f \in A[x]$ irreducible con $grd(f) \geqslant 1$ y sean $g, h \in A[x] \mid f | gh$

$$f \text{ es primitivo } \Rightarrow \text{ es irreducible en } K[x] \Rightarrow f \text{ es primo en } K[x]$$

Luego si $f|gh \Rightarrow f|g \ \vee \ f|h$ en $K[x]$.
Supongamos (lo cual no es restrictivo) que $f|g \Rightarrow \exists \phi \in K[x] \mid g = \phi f$

$$\phi = \frac{a}{b} f' \mid f' \in A[x] \text{ primitivo}$$

Luego $g = \frac{a}{b} f f' \Rightarrow bg = af'f \Rightarrow C(bg) = C(aff')$

$$C(bg) = bC(g) = aC(ff') = aC(f)C(f') = a$$

Luego $\frac{a}{b} = C(g) \in A \Rightarrow g = C(g) f f' \Rightarrow f|g$ en $A[x]$. □

4.3. Criterios básicos de irreducibilidad de polinomios

Sea K un cuerpo:
1) En $K[x]$, todo polinomio no nulo es asociado a un polinomio mónico:

$$\text{Sea } \phi = \sum_{i=0}^{n} a_i x^i \mid a_n \neq 0 \Rightarrow a_n \in U(K[x])$$

$$\psi = a_n^{-1}\phi = \sum_{i=0}^{n} a_n^{-1} a_i x^i \text{ es mónico}$$

Lema 4.18. *Dos polinomios mónicos son asociados $\Leftrightarrow$ son iguales.*

Demostración. Sean:

$$\phi = \sum_{i=0}^{n} a_i x^i \quad \psi = \sum_{i=0}^{m} b_i x^i \mid \phi, \psi \text{ mónicos}$$

ϕ y ψ son asociados $\Leftrightarrow \exists a \in K \setminus \{0\} \mid \phi = a\psi$
Que es decir que:

$$\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{m} a b_i x^i \Leftrightarrow n = m \ \wedge \ a_i = a b_i \ \forall i \in \{0, \ldots, n\}$$

En particular, como $a_n = b_m = 1 \Rightarrow 1 = a \Leftrightarrow \phi = \psi$ □

Por tanto, para conocer los polinomios irreducibles en $K[x]$ (salvo asociados), basta con conocer los irreducibles mónicos.

2) En $K[x]$ no hay irreducibles de grado 0, ya que todos los de grado 0 son unidades.

Proposición 4.19. *Todo polinomio de grado 1 en $K[x]$ es irreducible.*

Demostración. Sea $\phi \in K[x] \mid grd(\phi) = 1 \ \wedge \ \phi \notin U(K[x])$:
Sea ϕ' divisor de $\phi \Rightarrow \exists \phi'' \in K[x] \mid \phi = \phi'\phi''$ con $\phi', \phi'' \neq 0$.

$$1 = grd(\phi) = grd(\phi') + grd(\phi'') \Rightarrow \begin{cases} grd(\phi') = 0 & \Rightarrow \ \phi' \in U(K[x]) \\ \vee & \\ grd(\phi') = 1 & \Rightarrow \ grd(\phi'') = 0 \Rightarrow \\ \Rightarrow \phi'' \in U(K[x]) & \Rightarrow \ \phi' \sim \phi \end{cases}$$

Por lo que los únicos divisores de ϕ son los triviales $\Rightarrow \phi$ es irreducible. □

Los polinomios irreducibles mónicos de grado 1 en $K[x]$ son los de la forma:

$$\{x + a \mid a \in K\}$$

Si $K = \mathbb{Z}_p$ con p primo de $\mathbb{Z}$ mayor o igual que 2, son:

$$\{x, x+1, \ldots x+p-1\}$$

Teorema 4.20 (Teorema fundamental del Álgebra, Gauss)**.**
En $\mathbb{C}[x]$, los únicos polinomios irreducibles son los de grado 1.

Demostración. Excede el conocimiento del curso. □

Teorema 4.21 (de Ruffini)**.** *Sea $\phi \in K[x]$, $a \in A$. Entonces:*

$$\textit{El resto de dividir } \phi \textit{ entre } (x-a) \textit{ es } \phi(a)$$

Demostración. Dividimos ϕ entre $(x-a)$ y obtenemos que:

$$\phi = (x-a)\psi + r \mid r = 0 \ \vee \ grd(r) < grd(x-a) = 1$$

Por lo que sabemos que $r \in K$. Además:

$$\phi(a) = ((x-a)\psi + r)(a) = (a-a)\psi(a) + r = 0 + r = r$$

□

Proposición 4.22. *Sea $\phi \in K[x] \mid grd(\phi) \geqslant 2$:*

$$\phi \textit{ tiene un factor de grado } 1 \textit{ en } K[x] \Leftrightarrow \phi \textit{ tiene una raíz en } K$$

Demostración.
$\Longrightarrow$)

$$\exists \phi_1 = a_0 + a_1 x \in K[x] \mid \phi_1 \neq 0 \ \wedge \ \phi_1 | \phi \Rightarrow \exists \phi_2 \in K[x] \mid \phi = \phi_1 \phi_2$$

$$\phi = \phi_1 \phi_2 = (a_0 + a_1 x)\phi_2$$

Sea $a = -a_0 a_1^{-1}$:

$$\phi(a) = \phi_1(a)\phi_2(a) = (a_0 + a_1 a)\phi_2(a) = (a_0 + a_1(-a_0 a_1^{-1}))\phi_2(a) = 0$$

$\Longleftarrow$)

$$\exists a \in K \mid \phi(a) = 0$$

Por el Teorema de Ruffini (Teorema 4.21), tenemos que:

$$\phi = q(x-a) + \phi(a) = q(x-a) \Rightarrow x - a | \phi$$

□

Corolario 4.22.1 (Criterio de la raíz)**.** *de la Proposición 4.22.*
Sea $\phi \in K[x] \mid grd(\phi) \in \{2, 3\}$. Entonces:

$$\phi \textit{ es irreducible } \Leftrightarrow \phi \textit{ no tiene raíces en } K$$

Demostración.
Si ϕ es de grado 2, sus divisores propios serán de grado 1 o menos y sabemos por la Proposición 4.21 que no tiene de grado 1 y además, los polinomios de grado 0 son unidades, por lo que no serían factores propios.

Si ϕ es de grado 3, sus divisores propios serían de grado 2 o menos y por lo anterior sabemos que no pueden ser de grado 1 o menos, luego podría tener de grado 2, pero para que el producto en el que se divide sea de grado 3 haría falta un polinoimo de grado 1, imposible. □

Teorema 4.23. *En $\mathbb{R}[x]$, los polinomios irreducibles son los de grado 1 y los de grado 2 de la forma:*

$$ax^2 + bx + c \mid b^2 - 4ac < 0$$

Por tanto, los irreducibles mónicos en $\mathbb{R}[x]$ son:

$$\{x + a \mid a \in \mathbb{R}\} \cup \{x^2 + bx + c \mid b, c \in \mathbb{R} \ \wedge \ b^2 - 4c < 0\}$$

Notemos que pondemos listar todos los polinomios mónicos irreducibles de grado 2 ó 3 en $\mathbb{Z}_p[x]$, considerando todos los mónicos y quedándonos con los que no tengan raíces:

- Para $p = 2$, listamos $x^2 + bx + c \in \mathbb{Z}_2[x] \mid b, c \in \mathbb{Z}_2$:

$$a = 0 \Rightarrow \begin{cases} b = 0 & x^2 & \text{reducible} & (x^2)(0) = 0 \\ b = 1 & x^2 + 1 & \text{reducible} & (x^2 + 1)(1) = 0 \end{cases}$$

$$a = 1 \Rightarrow \begin{cases} b = 0 & x^2 + x & \text{reducible} & (x^2 + x)(1) = 0 \\ b = 1 & x^2 + x + 1 & \text{irreducible} & \text{no tiene raíces} \end{cases}$$

- Para $p = 3$, listamos $x^2 + bx + c \in \mathbb{Z}_3[x] \mid b, c \in \mathbb{Z}_3$:

$$a = 0 \Rightarrow \begin{cases} b = 0 & x^2 & \text{reducible} & (x^2)(0) = 0 \\ b = 1 & x^2 + 1 & \text{irreducible} & \text{no tiene raíces} \\ b = 2 & x^2 + 2 & \text{reducible} & (x^2 + 2)(2) = 0 \end{cases}$$

$$a = 1 \Rightarrow \begin{cases} b = 0 & x^2 + x & \text{reducible} & (x^2 + x)(2) = 0 \\ b = 1 & x^2 + x + 1 & \text{reducible} & (x^2 + x + 1)(1) = 0 \\ b = 2 & x^2 + 2 & \text{irreducible} & \text{no tiene raíces} \end{cases}$$

$$a = 2 \Rightarrow \begin{cases} b = 0 & x^2 + 2x & \text{reducible} & (x^2 + 2x)(0) = 0 \\ b = 1 & x^2 + 2x + 1 & \text{reducible} & (x^2 + 2x + 1)(2) = 0 \\ b = 2 & x^2 + 2x + 2 & \text{irreducible} & \text{no tiene raíces} \end{cases}$$

Para los polinomios de grado 4, los listamos y descartamos los que tengan raíces. Si no tienen raíces entonces no tienen factores de grado 1 $\Rightarrow$ no tienen factores de grado 3.
Puede tener de grado 2, luego cogemos el polinomio y lo dividimos entre irreducibles de grado 2.

Ejemplo.
1. Factorizar $f = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$.

$$f(0) = 1 = f(1) \Rightarrow f \text{ no tiene raíces } \Rightarrow f \text{ no tiene factores de grado 1}$$

Luego f tampoco tiene factores de grado 3. Puede tener de grado 2.

Como el único polinomio irreducible de grado 2 en $\mathbb{Z}_2[x]$ es x^2+x+1, dividimos entre él:

$$f = (x^2+x+1)(x^2+x+1)+x+1 \Rightarrow x^2+x+1 \not| f$$

Luego f no tiene factores de grado 2 $\Rightarrow$ f es irreducible al no tener factores de grado 1, 2 ni 3.

2. Factorizar $x^5+x^4+x^2+1 \in \mathbb{Z}_3[x]$.

$$f(0) = 1 = f(1) \quad f(2) = 2 \Rightarrow f \text{ no tiene raíes } \Rightarrow f \text{ no tiene factores de grado 1}$$

Luego f tampoco tiene factores de grado 4. Puede tener de grado 2 ó 3.

Buscamos factores irreducibles de grado 2, que pueden ser: x^2+1, x^2+x+2, x^2+2x+2.

$$f = (x^2+1)(x^3+x^2+2x)+x+1$$
$$f = (x^2+x+2)(x^3+x)+x+1$$
$$f = (x^2+2x+2)(x^2+2x)+2$$

Luego f no tiene factores de grado 2 $\Rightarrow$ f no tiene factores de grado 3.

Por tanto, f es irreducible.

3) Factorizar $f = x^7+2x^5+x^4+2x^3+x+2 \in \mathbb{Z}_3[x]$.

$$f(1) = 0 \Rightarrow x-1 = x+2 | f \Rightarrow f = (x+2)g \mid g = x^6+x^5+x^3+1$$

Factorizamos g:

$$g(2) = 0 \Rightarrow x-2 = x+1 | g \Rightarrow g = (x+1)h \mid h = x^5+x^2+2x+1$$

Factorizamos h:

$$h(0), h(1), h(2) \neq 0 \Rightarrow h \text{ no tiene raíces } \Rightarrow h \text{ no tiene factores de grado 1}$$

Luego tampoco tiene factores de grado 4. Buscamos factores de grado 2 en $\mathbb{Z}_3[x]$, que pueden ser:
x^2+1, x^2+x+2 ó x^2+2x+2.

$$h = (x^2+1)(x^3+2x+1)$$

Factorizamos x^3+2x+1:
No tiene raíces en $\mathbb{Z}_3[x]$ $\Rightarrow$ es irreducible por el Criterio de la Raíz (Corolario 4.22.1).

En resumen:

$$f = (x+2)(x+1)(x^2+1)(x^3+2x+1)$$

4.4. Polinomios en los anillos de enteros y de racionales cuadráticos

Recordemos que:
1) Los irreducibles de grado 0 en $\mathbb{Z}[x]$ son los irreducibles de $\mathbb{Z}$ (los números primos). En $\mathbb{Q}[x]$ no hay irreducibles de grado 0 por ser $\mathbb{Q}$ un cuerpo.
2) Sea $f \in \mathbb{Z}[x] \mid grd(f) > 0$ y sea f primitivo ($C(f) = 1$). Entonces:

$$f \text{ es irreducible en } \mathbb{Z}[x] \Leftrightarrow f \text{ es irreducible en } \mathbb{Q}[x]$$

3) Sea $\phi \in \mathbb{Q}[x] \mid grd(\phi) > 0$ y sea $\phi = \frac{a}{b} f \mid a, b \in \mathbb{Z},\ b \neq 0$ y f primitivo. Entonces:

$$\phi \text{ es irreducible en } \mathbb{Q}[x] \Leftrightarrow f \text{ es irreducible en } \mathbb{Z}[x]$$

Como todo polinomio de grado 1 en $\mathbb{Q}[x]$ es irreducible, entonces:
4) Un polinomio $f = a_0 + a_1 x \in \mathbb{Z}[x] \mid a_1 \neq 0$:

$$f \text{ es irreducible en } \mathbb{Z}[x] \Leftrightarrow mcd(a_0, a_1) = 1$$

Para grado 2 ó 3 sabemso que en $\mathbb{Q}[x]$ son irreducibles aquellos polinomios que no tienen raíces en $\mathbb{Q}$.
5) Un polinomio $f \in \mathbb{Z}[x]$ con $grd(f) \in \{2, 3\}$:

$$f \text{ es irreducible en } \mathbb{Z}[x] \Leftrightarrow f \text{ primitivo y no tiene raíces en } \mathbb{Q}$$

Proposición 4.24. *Sea* $f = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x] \mid n \geqslant 1$.
Sea $\frac{a}{b} \in \mathbb{Q} \mid f\left(\frac{a}{b}\right) = 0$ *y* $mcd(a, b) = 1$. *Entonces:*

$$(bx - a) \text{ es un divisor propio de } f \text{ en } \mathbb{Z}[x]$$

Es decir:

$$\exists g \in \mathbb{Z}[x] \mid f = (bx - a)g$$

Demostración.
Supongamos que $f\left(\frac{a}{b}\right) = 0$:
Por el Teorema de Ruffini (Teorema 4.21):

$$x - \frac{a}{b} | f \text{ en } \mathbb{Q}[x] \overset{b \in U(\mathbb{Q})}{\Longrightarrow} bx - a = b\left(x - \frac{a}{b}\right) | f \text{ en } \mathbb{Q}[x]$$

Por lo que $\exists g \in \mathbb{Q}[x] \mid f = (bx - a)g$
Sabemos que $g = \frac{c}{d} g' \mid c, d \in \mathbb{Z} \ \wedge \ d \neq 0 \ \wedge \ g'$ primitivo.

$$f = (bx - a)g = (bx - a)\frac{c}{d} g' \Rightarrow df = c(bx - a)g'$$

$$dC(f) = C(df) = C(c(bx - a)g') = cC((bx - a)g') = cC(bx - a)C(g') = c$$

Luego $dC(f) = c \Rightarrow \mathbb{Z} \ni C(f) = \frac{c}{d}$.

Por lo que $g = \frac{c}{d} g' = C(f)g' \in \mathbb{Z}[x]$. □

Corolario 4.24.1. *de la Proposición 4.24.*
Sea $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x] \mid n \geqslant 1$.
Sea $\frac{a}{b} \in \mathbb{Q} \mid f\left(\frac{a}{b}\right) = 0$ *y* $mcd(a,b) = 1$. *Entonces:*

$$a|a_0 \ \wedge \ b|a_n \text{ en } \mathbb{Z}[x]$$

Demostración.

$$f = (bx - a)g \in \mathbb{Z}[x]$$

Sea $g = b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$:

$$a_0 + a_1x + \ldots + a_nx^n = (bx - a)(b_0 + b_1x + \ldots + b_{n-1}x^{n-1})$$

Luego:

$$a_0 = -ab_0 = a(-b_0) \Rightarrow a|a_0$$

$$a_n = bb_{n-1} \Rightarrow b|a_n$$

□

Corolario 4.24.2. *del Corolario 4.24.1.*
1) Sea $f = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x] \mid n \geqslant 1$. *Entonces:*
Las raíces de f *en* $\mathbb{Q}$ *están en* $\mathbb{Z}$.
2) Sea $n \in \mathbb{Z} \mid \sqrt{n} \notin \mathbb{Z} \Rightarrow \sqrt{n} \notin \mathbb{Q}$.

Demostración.
1) Si $\frac{a}{b} \in \mathbb{Q} \mid f\left(\frac{a}{b}\right) = 0 \Rightarrow a|a_0 \ \wedge \ b|1 \Rightarrow b = \pm 1 \Rightarrow \frac{a}{b} = \pm a \in \mathbb{Z}$.

2) Sea $n \in \mathbb{Z} \mid \sqrt{n} \notin \mathbb{Z} \Rightarrow x^2 - n$ no tiene raíces en $\mathbb{Z} \Rightarrow^{1)}$ tampoco en $\mathbb{Q} \Rightarrow \sqrt{n} \notin \mathbb{Q}$. □

Ejemplo. Factorizar en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$ $f = 20x^4 - 10x^3 - 80x^2 + 80x - 20$.

$$C(f) = 10 \Rightarrow f = 10g \mid g = 2x^4 - x^3 - 8x^2 + 8x - 2 \text{ primitivo}$$

Factorizamos g:
Las posibles raíces en $\mathbb{Q}$ de g son de la forma: $\frac{a}{b} \mid a|a_0 = (-2) \ \wedge \ b|a_n = 2$.
Luego las opciones son: ± 1, ± 2, $\pm 1/2$. Evaluamos en ellos y obtenemos que:

$$g\left(\frac{1}{2}\right) = 0 \Rightarrow 2x - 1|g \text{ en } \mathbb{Z}[x]$$

Dividimos entre $2x - 1$:

$$g = (2x - 1)(x^3 - 4x + 2)$$

$2x - 1$ es irreducible en $\mathbb{Z}[x]$ por ser de grado 1 y primitivo.
Buscamos raíces de $x^3 - 4x + 2$ que sabemos que son enteras, por ser mónico:
Sus posibles raíces son de la forma $\frac{a}{b} \mid a|a_0 = 2 \ \wedge \ b|a_n = 1$.
Luego las opcinoes son: ± 1 y ± 2. Evaluamos en ellos y ninguna es raíz.

Por tanto, tenemos que $x^3 - 4x + 2$ es irreducible por ser primitivo y no tener raíces en $\mathbb{Q}$.

La factorización de f en $Z[x]$ es:

$$f = 2 \cdot 5(2x-1)(x^3 - 4x + 2)$$

Mientras que en $\mathbb{Q}[x]$ es:

$$f = 10(2x-1)(x^3 - 4x + 2) \quad (10 \in U(\mathbb{Q}[x]))$$

$$f = 20\left(x - \frac{1}{2}\right)(x^3 - 4x + 2)$$

Ejemplo. Factorizar en $\mathbb{Q}[x]$: $\phi = x^3 + \frac{1}{2}x^2 - x - 3$

$$\phi = \frac{1}{2}(2x^3 + x^2 - 2x - 6) = \frac{1}{2}f \mid f \in \mathbb{Z}[x] \text{ primitivo}$$

Las posibles raíces de f son de la forma $\frac{a}{b} \mid a|a_0 = -6 \ \wedge \ b|a_n = 2$.
Luego las opciones son: ± 1, ± 2, ± 3, ± 6, $\pm 1/2$ ó $\pm 3/2$. Evaluando, llegamos a que:

$$f\left(\frac{3}{2}\right) = 0 \Rightarrow (2x-3)|f \text{ en } \mathbb{Z}[x] \Rightarrow f = (2x-3)(x^2 + 2x + 2)$$

$2x - 3$ es irreducible en $\mathbb{Q}[x]$ por ser de grado 1.
$x^2 + 2x + 2$, sus posibles raíces son de la forma $\frac{a}{b} \mid a|a_0 = 2 \ \wedge \ b|a_n = 1$.
Luego las opciones son: ± 1, ± 2. Evaluando, ninguna es raíz, por lo que $x^2 + 2x + 2$ no tiene raíces en $\mathbb{Q}$. Luego es irreducible.

$$\phi = \frac{1}{2}(2x-3)(x^2 + 2x + 2) = \left(x - \frac{3}{2}\right)(x^2 + 2x + 2)$$

4.4.1. Criterio de reducción

Sea $p \in \mathbb{Z} \mid p \geqslant 2$ primo y consideramos el homomorfismo de anillos:

$$R_p : \mathbb{Z} \Rightarrow \mathbb{Z}_p \qquad R_p(a) := R(a; p)$$

Que induce un homomorfismo (visto ya en el Ejemplo **??**):

$$R_p : \mathbb{Z}[x] \Rightarrow \mathbb{Z}_p[x] \qquad R_p\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} R_p(a_i)x^i$$

Con $grd(R_p(f)) \leqslant grd(f)$

Proposición 4.25 (Criterio de reducción)**.**
Sea $f \in \mathbb{Z}[x] \mid grd(f) > 0 \ \wedge \ grd(f) = grd(R_p(f))$
Supongamos que $R_p(f)$ *no tiene factores de grado* r *siendo* $0 < r < grd(f)$ *en* $\mathbb{Z}_p[x]$.
Entonces:

$$f \text{ no tiene factores de grado } r \text{ en } \mathbb{Z}[x]$$

En particular, si $R_p(f)$ *es irreducible en* $\mathbb{Z}_p[x] \Rightarrow f$ *es irreducible en* $\mathbb{Z}[x]$.

Demostración.
Supongamos que $f \in \mathbb{Z}[x] \mid grd(f) > 0 \ \wedge \ grd(f) = grd(R_p(f))$ y que $R_p(f)$ no tiene factores de grado r siendo $0 < r < grd(f)$ en $\mathbb{Z}_p[x]$.

Supongamos que $\exists g \in \mathbb{Z}[x] \mid grd(g) = r \ \wedge \ g|f$ en $\mathbb{Z}[x]$.
Entonces, $\exists h \in \mathbb{Z}[x] \mid f = gh \ \wedge \ s = grd(h) \Rightarrow grd(f) = grd(g) + grd(h) = r + s$

$$R_p(f) = R_p(gh) = R_p(g)R_p(h) \mid grd(R_p(g)) \leqslant r \ \wedge \ grd(R_p(h)) \leqslant s$$

Entonces:

$$r + s = grd(R_p(f)) = grd(R_p(g)) + grd(R_p(h)) \leqslant r + s \Rightarrow$$

$$\Rightarrow grd(R_p(g)) = r \ \wedge \ grd(R_p(h)) = s$$

Luego $R_p(g)$ es un factor de grado r de $R_p(f)$. Contradicción con la hipótesis.

Luego f no tiene factores de grado r en $\mathbb{Z}[x]$. □

Proposición 4.26 (Criterio de Eisenstein)**.** *Sea $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x] \mid grd(f) > 0$ y sea f primitivo.*
Entonces, f es irreducible en $\mathbb{Z}[x]$ (y también en $\mathbb{Q}[x]$) si:

$$\exists p \in \mathbb{Z} \mid p \geqslant 2 \text{ primo}$$

Tal que verifica alguna de las siguientes condiciones:
i) $p|a_i \ \ \forall i \in \{0, \ldots, n-1\} \ \wedge \ p^2 \nmid a_0$
ii) $p|a_i \ \ \forall i \in \{1, \ldots, n\} \ \wedge \ p^2 \nmid a_n$

Demostración.
i) Supongamos que se verifica i) y sin embargo, que f es reducible:
Luego $f = gh \mid g, h \in \mathbb{Z}[x] \ \wedge \ grd(g) = r \geqslant 1 \ \wedge \ grd(g) = s \geqslant 1$.
Sean $g = b_0 + b_1x + \ldots b_rx^r$ y $h = c_0 + c_1x + \ldots + c_sx^s$.
Como $a_0 = b_0c_0$ y $p|a_0 \Rightarrow p|b_0c_0 \Rightarrow p|b_0 \ \vee \ p|c_0$.
Como $p^2 \nmid a_0 \Rightarrow p$ no puede dividir simultáneamente a los dos.
Supongamos (lo cual no es resitrictivo) que $p|b_0 \ \wedge \ p \nmid c_0$:
Como f es primitivo:

$$\left.\begin{array}{l} mcd(a_0, a_1, \ldots, a_{n-1}, a_n) = 1 \\ p|a_i \ \ \forall i \in \{0, \ldots, n-1\} \end{array}\right\} \Rightarrow p \nmid a_n$$

Como $a_n = b_rc_s$, entonces $p \nmid b_rc_s \Rightarrow p \nmid b_r \ \wedge \ p \nmid c_s$.
Sea b_i el primer coeficiente tal que $p \nmid b_i$ con $0 < i \leqslant r < n$.
Consideramos el coeficiente i-ésimo de f: a_i:

$$a_i = b_0c_i + b_ic_{i-1} + \ldots + b_{i-1}c_1 + b_ic_0$$

$$p|a_i(i < n) \Rightarrow p(b_0c_i + b_ic_{i-1} + \ldots + b_{i-1}c_1 + b_ic_0) \Rightarrow p|b_ic_0$$

Pero $p \nmid b_i$ y $p \nmid c_0$. Contradicción con que p es primo.

Luego $f \neq gh \Rightarrow f$ es irreducible.

□