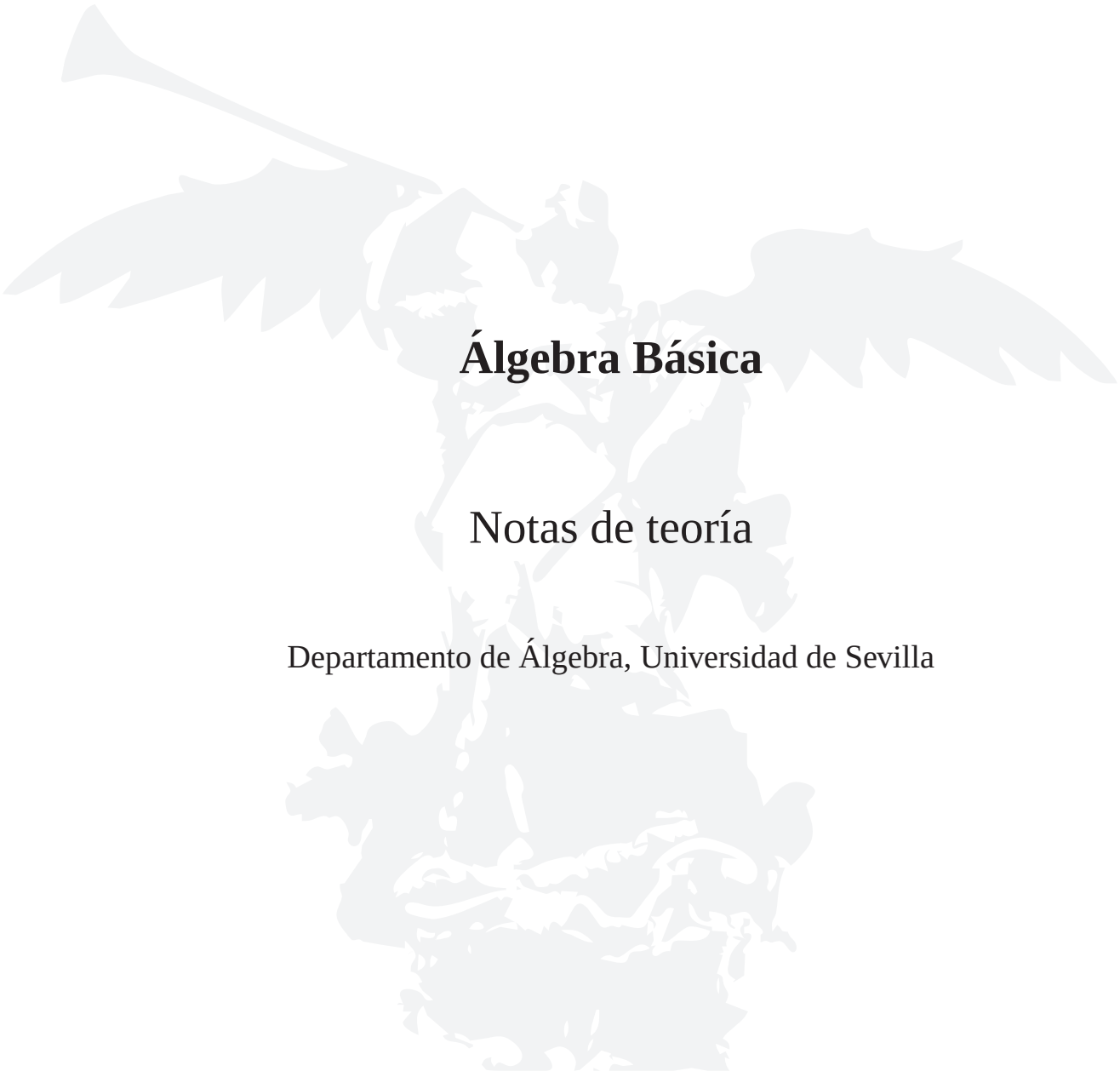


Álgebra Básica

Notas de teoría

Departamento de Álgebra, Universidad de Sevilla

Índice

Tema 1. Lenguaje y Matemáticas. Conjuntos.

Antes de comenzar decir que supondremos que todos sabemos qué son los números (naturales, enteros, racionales y reales), y que conocemos las propiedades elementales de la suma y el producto de números (asociativa, conmutativa, distributiva,..) La notación que usaremos a lo largo del curso será:

- Los números naturales, $\mathbf{N}$.
- Los números enteros, $\mathbf{Z}$.
- Los números racionales, $\mathbf{Q}$.
- Los números reales, $\mathbf{R}$.

1.1. Introducción a la lógica proposicional.

En este tema trataremos de desarrollar el uso del lenguaje en el contexto de las matemáticas. A lo largo del mismo, por una *proposición* o sentencia lógica entenderemos una declaración que puede ser verdadera o falsa. Por ejemplo:

1) Hoy es lunes.
2) 3 es mayor que 7.
3) He nacido en Sevilla.

En los tres ejemplos es claro (aunque el 3 sea más complicado comprobarlo) que la declaración correspondiente es verdadera o falsa. Ésta es la característica fundamental de las proposiciones. La siguiente declaración (paradoja) “esta frase es falsa” no puede ser ni verdadera ni falsa, por tanto no la consideraremos como proposición.

Otros ejemplos de declaraciones que no son proposiciones son:

1) El color azul es bonito.
2) n es un número par.
3) ¿Quién ha llegado?

Consideremos el conjunto $\mathcal{P}$ de todas la proposiciones posibles. Este conjunto está dividido en dos partes: las proposiciones que son verdaderas y las proposiciones que son falsas. Lo que pretendemos ver ahora es cómo podemos combinar proposiciones para obtener otras nuevas y, además, estudiar cómo se traduce la veracidad o falsedad de las proposiciones combinadas en la proposición resultante. Generalmente usaremos las letras $p, q, r, ...$ para representar las proposiciones. Por ejemplo

$$p : \text{Hoy es lunes.}$$

Definición (Negación).– Dada una proposición p, definimos la proposición $\neg p$ (no p) como la proposición que es falsa cuando p es verdadera, y verdadera si p es falsa.

Esta definición se puede ilustrar en su *tabla de verdad*. Una tabla de verdad es la relación exhaustiva de todos los casos posibles de veracidad y falsedad que pueden darse en cada elemento de una proposición.

p	$\neg p$
V	F
F	V

Definición (Conjunción).– Dadas dos proposiciones p y q, definimos $p \wedge q$ (p y q) como la proposición que es verdadera sólo cuando ambas, p y q, son verdaderas. Su tabla de verdad es:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Definición (Disyunción).– Dadas dos proposiciones p y q, definimos la proposición $p \vee q$ (p o q) como aquélla que es verdadera cuando una o ambas proposiciones son verdaderas. Su tabla de verdad es:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Definición (Implicación).– Dadas dos proposiciones p y q, definimos la proposición $p \rightarrow q$ (p implica q) como la proposición que es falsa cuando p es verdadera y q falsa, y verdadera en los demás casos. Llamaremos a p la hipótesis y a q la conclusión. Su tabla de verdad es:

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Ya podemos construir numerosos ejemplos de proposiciones, y sus tablas de verdad. Por ejemplo, la tabla de verdad de la proposición $\neg p \vee q$ es

p	q	$\neg p \vee q$
V	V	V
V	F	F
F	V	V
F	F	V

Otro ejemplo algo más complicado: la tabla de verdad de $(p \wedge q) \rightarrow r$

p	q	r	$p \wedge q$	$(p \wedge q) \rightarrow r$
V	V	V	V	V
V	V	F	V	F
V	F	V	F	V
V	F	F	F	V
F	V	V	F	V
F	V	F	F	V
F	F	V	F	V
F	F	F	F	V

Se observa que las tablas de verdad de la implicación y del primer ejemplo coinciden.

Definición.– Diremos que dos proposiciones son *lógicamente equivalentes* si tienen la misma tabla de verdad.

Ejemplos.– Los siguientes pares de proposiciones son lógicamente equivalentes:

a) $p \vee (q \wedge r)$, $(p \vee q) \wedge (p \vee r)$ (propiedad distributiva)
b) $p \vee (q \vee r)$, $(p \vee q) \vee r$ (propiedad asociativa)

Definición.– Diremos que una proposición es una tautología si los valores de su tabla de verdad son todos verdaderos.

Por ejemplo $p \vee \neg p$. La negación de una tautología se denomina contradicción. Es decir, una contradicción es una proposición en cuya tabla de verdad sólo aparece el valor falso. Por ejemplo $p \wedge \neg p$.

Definición.– Dadas dos proposiciones p y q definimos la proposición $p \leftrightarrow q$ (p sí y sólo si q) como la proposición que es verdadera cuando p y q son ambas verdaderas ó ambas falsas.

Su tabla de verdad es:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Con esta definición se puede comprobar que dos proposiciones p y q son lógicamente equivalentes ($\Longleftrightarrow$) si la proposición $p \leftrightarrow q$ es una tautología.

Para terminar esta sección veamos cómo actúa la negación sobre $\vee$, $\wedge$ y $\rightarrow$. Es un fácil ejercicio comprobar que:
1) $\neg(p \vee q) \Longleftrightarrow \neg p \wedge \neg q$.
2) $\neg(p \wedge q) \Longleftrightarrow \neg p \vee \neg q$.

Estas propiedades se conocen con el nombre de las leyes de DeMorgan. Para ver cómo actúa la negación sobre $\rightarrow$ basta tener en cuenta que $p \rightarrow q \Leftrightarrow \neg p \vee q$, y aplicando las leyes de DeMorgan, tenemos que:

$$\neg(p \rightarrow q) \iff \neg(\neg p \vee q) \iff (\neg\neg p) \wedge \neg q \iff p \wedge \neg q$$

1.2. Conjuntos. Operaciones básicas.

Definición.– Llamaremos *conjunto* a una colección de objetos que comparten una propiedad. Para que un conjunto esté bien definido debe ser posible discernir si un objeto arbitrario está o no en él.

Los conjuntos pueden definirse de manera explícita, citando todos sus elementos entre llaves, por ejemplo

$$A = \{1, 2, 3, 4, 5\},$$

o de manera implícita, dando una (o varias) característica(s) que determine(n) si un objeto dado está o no en el conjunto, por ejemplo

$$A = \{x \mid x \text{ es un número natural par}\},$$

que se leerá: "A es el conjunto formado por los x tales que x es un número natural par". Esta última opción (la definición implícita) es obviamente imprescindible cuando el conjunto en cuestión tiene una cantidad infinita de elementos.

Notación.– Los conjuntos se notarán con letras mayúsculas: A, B,... y los elementos con minúsculas, en general. Si el elemento a pertenece al conjunto A escribiremos $a \in A$. En caso contrario escribiremos $a \notin A$.

Observación.– En ocasiones hay que considerar varios conjuntos en pie de igualdad. En estos casos es frecuente denotar los distintos conjuntos con la misma letra y un subíndice que los diferencia. Los subíndices pueden ser finitos y concretos, por ejemplo,

$$X_1, X_2, X_3, X_4, X_5;$$

finitos pero en cantidad desconocida,

$$X_1, X_2, ..., X_n,\ n \in \mathbf{N},$$

o arbitrarios; un ejemplo de esto sería considerar

$$\{A_i\}_{i \in I},$$

que se leería: la familia de conjuntos A_i donde i pertenece a I. Aquí I es el conjunto de subíndices que puede o no ser finito (por ejemplo I podría ser todo $\mathbf{N}$).

Definición.– Un conjunto que carece de elementos se denomina el *conjunto vacío* y se denota por $\emptyset$. Un conjunto con un único elemento se denomina unitario.

Notemos que, si $X = \{x\}$ es un conjunto unitario, debemos distinguir entre el conjunto X y el elemento x.

Definición.– Dados dos conjuntos A y B, si todo elemento de A es a su vez elemento de B diremos que A es un *subconjunto* de B y lo notaremos $A \subset B$. En caso contrario se notará $A \not\subset B$.

Proposición.– Sean A, B y C tres conjuntos cualesquiera. Se tienen las siguientes propiedades:

(a) $A \subset A, \emptyset \subset A$.

(b) Si $A \subset B$ y $B \subset A$, entonces $A = B$.

(c) Si $A \subset B$ y $B \subset C$, entonces $A \subset C$.

Demostración.– La primera propiedad se sigue directamente de la definición.

Para probar (b), fijémonos en que dos conjuntos son iguales si tienen exactamente los mismos elementos. Pero esto es tanto como decir que todos los elementos de A están en B, y viceversa; eso es que $A \subset B$ y $B \subset A$.

La demostración de (c) se sigue de la definición de subconjunto: todo elemento de A está en B, por ser $A \subset B$ y, dado que es elemento de B, está en C por ser $B \subset C$. Así todo elemento de A está en C y hemos finalizado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Dado dos conjuntos $A \subset X$ se define el *complementario* de A en X (o simplemente el complementario de A, si el conjunto X no se presta a confusión) como

$$X \setminus A = \{x \mid x \in X,\, x \notin A\},$$

esto es, el conjunto de elementos de X que no están en A. Otras notaciones que se pueden encontrar para $X \setminus A$ (donde X se obvia) son $\overline{A}$ o cA.

Observación.– Dados $A \subset X$, se dan las siguientes igualdades:

$$\overline{\emptyset} = X,\ \overline{X} = \emptyset,\ \overline{\overline{A}} = A.$$

Nos detendremos solamente en la tercera de las anteriores propiedades. En efecto, por definición

$$\overline{\overline{A}} = \{x \mid x \in X,\, x \notin \overline{A}\},$$

pero para un $x \in X$, $x \notin \overline{A}$ si y sólo si $x \in A$, por tanto los elementos de $\overline{\overline{A}}$ son precisamente los de A.

Notación.– Cuando A es un conjunto finito, el número de elementos de A se denomina cardinal de A y se notará $\sharp(A)$.

Definición.– Dados dos conjuntos A y B se define la *unión* de A y B, notado $A \cup B$ como el conjunto formado por aquéllos elementos que pertenecen al menos a uno de los dos conjuntos, A ó B.

Se definen de forma equivalente la unión de una cantidad finita de conjuntos $A_1, ..., A_n$, que denotaremos

$$A_1 \cup ... \cup A_n = \bigcup_{i=1}^{n} A_i,$$

y la unión de una familia arbitrariamente grande de conjuntos $\{A_i\}_{i\in I}$, que denotaremos

$$\bigcup_{i\in I} A_i.$$

Proposición.– La unión de conjuntos verifica las siguientes propiedades, para cualesquiera conjuntos A, B y C:

(a) Conmutativa: $A \cup B = B \cup A$.

(b) Asociativa: $(A \cup B) \cup C = A \cup (B \cup C)$.

(c) $\emptyset \cup A = A$.

Demostración.– Todas las pruebas son sencillas, y son un buen ejercicio para que el alumno comience a tratar de plasmar demostraciones rigurosas. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Dados dos conjuntos A y B se define la *intersección* de A y B, notado $A \cap B$, como el conjunto formado por aquéllos elementos que pertencen al mismo tiempo a ambos conjuntos, A y B.

Se definen de forma equivalente la intersección de una cantidad finita de conjuntos $A_1, ..., A_n$, y la intersección de una familia arbitrariamente grande de conjuntos $\{A_i\}_{i\in I}$, que denotaremos, respectivamente,

$$A_1 \cap ... \cap A_n = \bigcap_{i=1}^{n} A_i, \text{ y } \bigcap_{i\in I} A_i.$$

Si A y B son dos conjuntos tales que $A \cap B = \emptyset$ se dice que A y B son disjuntos.

Proposición.– La intersección de conjuntos verifica las siguientes propiedades, para cualesquiera conjuntos A, B y C:

(a) Conmutativa: $A \cap B = B \cap A$.

(b) Asociativa: $(A \cap B) \cap C = A \cap (B \cap C)$.

(c) $\emptyset \cap A = \emptyset$.

Demostración.– Las demostraciones se dejan como ejercicios. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

1.3. Cuantificadores universales y existenciales.

Los cuantificadores son elementos que nos permiten enunciar proposiciones (por ahora, relativas a conjuntos), de forma concisa y clara. Comenzaremos escribiendo una proposición de distintas formas. Por ejemplo, sabemos (lo probaremos más adelante) que:

La desigualdad $n^2 < 2^n$ es cierta para todos los naturales mayores o iguales que 5.

Podemos expresar (escribir) esta proposición de distintas formas:

- Para todo número natural n, si $n \geq 5$, entonces $n^2 < 2^n$.
- Para todo n, si $n \in \mathbf{N}$ y $n \geq 5$, entonces $n^2 < 2^n$.
- $(\forall n)[(n \in \mathbf{N} \wedge n \geq 5) \rightarrow (n^2 < 2^n)]$.

Cada vez que hemos escrito la proposición, hemos aumentado el grado de formalidad. En la última aparece el símbolo $\forall$ (para todo), que denominaremos *cuantificador universal*. Veamos otro ejemplo:

- Todos los elementos del conjunto B son negativos.
- Para todo $x \in B$, $x < 0$.
- $(\forall x \in B)(x < 0)$.
- Para todo x, si $x \in B$, entonces $x < 0$.
- $(\forall x)(x \in B \rightarrow x < 0)$.

La forma más general para una proposición conteniendo en cuantificador universal sería como sigue. Si $P(x)$ es una propiedad expresada en términos de x, entonces una proposición general con el cuantificador universal sería:

$$(\forall x)(P(x)),$$

que leeríamos: para todo x, (opcionalmente: se tiene, se verifica) $P(x)$.

Volvamos al primer ejemplo. Sabemos que la desigualdad $n^2 < 2^n$ es cierta si $n \geq 5$, pero no lo es si $2 \leq n \leq 4$. Es decir, sabemos que

- Existe un número natural n tal que $n^2 \geq 2^n$.
- Existe n tal que $n \in \mathbf{N}$ y $n^2 \geq 2^n$.
- $(\exists n)(n \in \mathbf{N} \wedge n^2 \geq 2^n)$.

El símbolo $\exists$ se lee como “existe” y se denomina *cuantificador existencial*.

Otro ejemplo:

- Algún elemento del conjunto B es positivo.
- Existe $x \in B$, $x > 0$.
- $(\exists x \in B)(x > 0)$.
- Existe x tal que $x \in B$ y $x > 0$.
- $(\exists x)(x \in B \wedge x > 0)$.

Si $P(x)$ es una propiedad expresada en términos de x, entonces una proposición general con el cuantificador existencial sería:

$$(\exists x)(P(x)),$$

que leeríamos: existe un x tal que $P(x)$.

Veamos un ejemplo con los dos cuantificadores:

- Existe un elemento del conjunto A que es menor que todos los elementos del conjunto B.
- Existe $x \in A$ tal que $x < y$ para todo $y \in B$.
- Existe $x \in A$ tal que, para todo $y \in B$, $x < y$.
- $(\exists x \in A)(\forall y \in B)(x < y)$.

En matemáticas también usamos el símbolo $\exists!$, que significa "existe un único". La expresión $(\exists! x)(P(x))$ se lee: "existe un único x tal que $P(x)$". Por ejemplo: $\exists! n \in \mathbf{N}$ tal que $n^3 = 8$.

Las proposiciones con cuantificadores se niegan siguiendo las dos reglas siguientes:

$$\neg[(\forall x)(P(x))] \Longleftrightarrow (\exists x)(\neg P(x))$$

$$\neg[(\exists x)(P(x))] \Longleftrightarrow (\forall x)(\neg P(x)).$$

Un ejemplo con los dos cuantificadores: la negación de

$$(\forall \epsilon > 0)(\exists n \in \mathbf{N})(1/n < \epsilon)$$

es

$$(\exists \epsilon > 0)(\forall n \in \mathbf{N})(1/n \geq \epsilon).$$

1.4. Demostraciones.

En esta sección veremos los tipos más importantes de demostraciones que usaremos a lo largo de todo el curso.

Prueba directa

Esquema:

Teorema.– Si p entonces q.

Demostración: Supongamos p. Entonces [...], se tiene q.

Proposición.– Sea n un número natural. Probar que si n es impar entonces n^2 es impar.

Demostración.– Si n es impar, es de la forma $n = 2k+1$. Por tanto $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, es decir, n^2 es impar. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Prueba de una proposición lógicamente equivalente.

Consiste en sustituir la proposición a demostrar por otra que sea lógicamente equivalente y tratar de probar esta última. Por ejemplo, si queremos probar que $p \to (q \vee r)$ podemos usar que es lógicamente equivalente a $(p \wedge \neg q) \to r$.

Esquema:

Teorema.– $p \to (q \vee r)$.

Demostración: Supongamos $p \wedge \neg q$. Entonces [...], se tiene r.

Prueba del contrarrecíproco.

Es un caso particular de la anterior. Si se quiere probar $p \to q$, usamos que es lógicamente equivalente a $\neg q \to \neg p$, y

Esquema:

Teorema $p \to q$.

Demostración: Supongamos $\neg q$. Entonces [...], se tiene $\neg p$.

Proposición.– Sea n un número natural. Probar que si n^2 es impar entonces n es impar.

Demostración.– Supongamos que n es par, es decir $n = 2k$. Entonces $n^2 = 4k^2$ es par. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Prueba por reducción al absurdo.

Si queremos probar que p es un teorema (es verdadero), lo que queremos ver es que p es una tautología. Por tanto $\neg p$ es una contradicción.

Esquema:

Teorema.– p.

Demostración: Supongamos $\neg p$. Entonces [...], que es falso. Luego es una contradicción. Se tiene p.

Proposición (Pitágoras).– $\sqrt{2}$ no es racional.

Demostración.– Supongamos que $\sqrt{2}$ es racional, es decir, $\sqrt{2} = m/n$, y suponemos que m y n no tienen ningún factor común. Elevando al cuadrado tenemos $2 = m^2/n^2$, luego $m^2 = 2n^2$. Como m^2 es un número par, se deduce (probarlo) que m es par, $m = 2r$. Sustituyendo tenemos $4r^2 = 2n^2$, luego $2r^2 = n^2$, de donde deducimos que n^2, y por tanto n, es un número par. Esto contradice el hecho de que m y n no tenían factores comunes. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Contraejemplos.

Supongamos que tenemos una proposición y queremos saber si es verdadera o falsa. Por ejemplo, sea $P(n)$ una propiedad que tratamos probar que se verifica para todos los números naturales n. Entonces:

- Si $P(n)$ es verdadera, tenemos que dar una prueba general.
- Si $P(n)$ es falsa, basta dar un valor de n en el que no se verifique la propiedad.

Ejemplo.– Si nuestra propiedad $P(n)$ es: "todo número impar es primo", basta comprobar que para $n = 9$ no se verifica la propiedad, luego es falsa.

Prueba por inducción.

Supongamos que tratamos de probar una propiedad (un enunciado) sobre los números naturales $n \geq n_0$, para un n_0 dado. Si denotamos por $P(n)$ dicha propiedad, la prueba por inducción funciona de la siguiente manera:

Esquema:

Teorema.– $P(n)$.

Demostración: Probar que $P(n_0)$ es cierta.

Suponer que $P(n)$ es cierta (hipótesis de inducción).

Probar que $P(n+1)$ es cierta.

El segundo paso se puede sustituir por

2') Suponer que $P(k)$ es cierta $\forall k, n_0 \leq k \leq n$. Esta versión alternativa se conoce como *inducción fuerte*.

Proposición.– $\forall n \in \mathbf{N}$ se verifica que

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Demostración.– Sigamos los pasos.

1) El resultado se verifica para $n = 1$, pues $1 = 1(1+1)/2$.

2) Suponemos el resultado cierto para n, es decir, $1 + 2 + \ldots + n = n(n+1)/2$.

3) Tenemos que probar que $1 + 2 + \ldots + n + (n+1) = (n+1)(n+2)/2$. En efecto,

$$1+2+\ldots+n+(n+1) = [1+2+\ldots+n]+(n+1) = \frac{n(n+1)}{2}+(n+1) = \frac{(n+1)(n+2)}{2}.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Proposición.– Todo número natural $n > 1$ tiene un divisor primo.

Demostración.– Usaremos ahora la inducción fuerte.

1) El resultado se verifica para $n = 2$, pues 2 es un divisor primo de 2.

2') Suponemos el resultado cierto $\forall k, n_0 \leq k < n$.

3) Tenemos que probar que n tiene un divisor primo. Si n es primo, n es el divisor buscado. Si n no es primo entonces $n = rs$, con $1 < r, s < n$. Luego r (y s) tiene un divisor primo. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Prueba por doble inclusión.

Este tipo es el más habitual en teoría de conjuntos y se basa en el resultado de la sección anterior que afirma que si A y B son conjuntos verificando $A \subset B$ y $B \subset A$, entonces $A = B$.

Esquema:

Teorema.– $A = B$.

Demostración: Sea $x \in A$ cualquiera, probar que $x \in B$ (esto demuestra $A \subset B$).

Sea $x \in B$ cualquiera, probar que $x \in A$ (esto demuestra $B \subset A$).

En la próxima sección veremos algunos ejemplos de esta técnica.

1.5. Subconjuntos.

Veremos ahora algunas propiedades más de los conjuntos y demostraremos algunos resultados fundamentales utilizando la técnica de la doble inclusión.

Definición.– Dado un conjunto X, se define el *conjunto de las partes* de X, notado $\mathcal{P}(X)$, como el conjunto cuyos elementos son todos los subconjuntos de X.

Ejemplo.– Si tenemos el conjunto $X = \{0, 1, 2, 3\}$, entonces

$$\begin{aligned}\mathcal{P}(X) \;=\; \{\,&\emptyset,\ \{0\},\ \{1\},\ \{2\},\ \{3\},\{0,1\},\ \{0,2\},\ \{0,3\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\\ &\{0,1,2\},\ \{0,1,3\},\ \{0,2,3\},\ \{1,2,3\},\ X\,\}\end{aligned}$$

Proposición.– El conjunto $\mathcal{P}(X)$ es finito si y sólo si lo es X. De hecho, en este caso,

$$\sharp\left(\mathcal{P}(X)\right) = 2^{\sharp(X)}.$$

Demostración.– En cuanto a la primera afirmación, si X es infinito, lo es obviamente $\mathcal{P}(X)$. La otra implicación viene dada por la fórmula sobre los cardinales que probaremos por inducción.

El caso $\sharp(X) = 0$ es elemental, porque entonces $X = \emptyset$ y, por tanto $\mathcal{P}(X) = \{\emptyset\}$. Notemos que $\mathcal{P}(X)$ no es el conjunto vacío, es un conjunto unitario, cuyo único elemento es el conjunto vacío.

Supuesto cierto el resultado para todos los conjuntos que tienen, pongamos, n elementos, tomemos X un conjunto de n elementos, $x \in X$ cualquiera, y escribamos

$$X = X' \cup \{x\},$$

donde $X' = X \setminus \{x\}$ tiene $n-1$ elementos. Entonces es claro que los subconjuntos de X son, bien subconjuntos de X', bien subconjuntos de X' a los que se ha añadido x. Dado que, por hipótesis de inducción,

$$\sharp\left(\mathcal{P}\left(X'\right)\right) = 2^{n-1}$$

se tiene, por tanto,

$$\sharp\left(\mathcal{P}(X)\right) = 2 \cdot 2^{\sharp(\mathcal{P}(X'))} = 2 \cdot 2^{n-1} = 2^n.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

El comportamiento de los subconjuntos con las operaciones habituales entre conjuntos es bastante intuitivo. De hecho, tanto la unión como la intersección se pueden usar para caracterizar a los subconjuntos (esto es, dar una propiedad que verifican los subconjuntos de un conjunto dado, y solamente éstos).

Proposición.– La unión de conjuntos verifica las siguientes propiedades, para cualesquiera conjuntos A, B y C:

(a) $A \subset B \iff A \cup B = B$.

(b) Si $A \subset B$, entonces $A \cup (B \setminus A) = B$.

Demostración.– Ambas pruebas son sencillas. Como ilustración de cómo se ataca una doble implicación, probaremos (a).

Comenzaremos suponiendo que $A \subset B$. Entonces todos los elementos de A están en B, por tanto $A \cup B = B$ de manera inmediata. Recíprocamente, supongamos que $A \cup B = B$. Entonces todo elemento que esté en A ó en B está forzosamente en B, con lo que se tiene $A \subset B$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Proposición.– La intersección de conjuntos verifica las siguientes propiedades, para cualesquiera conjuntos A, B y C:

(a) $A \subset B \iff A \cap B = A$.

(b) Si $A \subset B$, entonces $A \cap (B \setminus A) = \emptyset$.

Demostración.– Las demostraciones se dejan como ejercicios. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Terminamos el tema enunciando dos resultados fundamentales de la teoría de conjuntos, cuyas demostraciones son buenos ejemplos del uso de la doble inclusión como técnica de demostración.

Proposición.– Dados tres conjuntos A, B y C se verifican las siguientes igualdades:

(a) Leyes distributivas:

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

(b) Leyes de De Morgan (supongamos $A, B \subset C$):

$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B), \quad C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$$

Demostración.– Probaremos una de las leyes distributivas y una de las leyes de De Morgan; las restantes quedan como ejercicio por ser simétricas a las probadas. Ambos resultados se probarán por doble inclusión.

Veamos que $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$. Para ello tomemos un elemento arbitrario $x \in A \cap (B \cup C)$. Esto quiere decir que x está en A y además en B ó en C. Esto implica que, bien está en $A \cap B$, bien está en $A \cap C$. En cualquier caso $x \in (A \cap B) \cup (A \cap C)$.

Demostremos ahora que $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Si consideramos un elemento cualquiera $y \in (A \cap B) \cup (A \cap C)$, y ha de pertencer a $A \cap B$ o a $A \cap C$. Por tanto, bien está en A y en B o en A y en C. En cualquier circunstancia ha de estar en A y al menos en uno de los otros dos conjuntos B ó C. De aquí $y \in A$ y además $y \in B \cup C$.

Pasemos a probar la segunda ley de De Morgan. Veamos primero $C \setminus (A \cap B) \subset (C \setminus A) \cup (C \setminus B)$. Un elemento x de $C \setminus (A \cap B)$ ha de estar en C, pero no en $A \cap B$, por lo que no puede estar en al menos uno de los dos conjuntos A ó B. Así, x ha de pertenecer, bien a $C \setminus A$, bien a $C \setminus B$. En cualquier caso $x \in (C \setminus A) \cup (C \setminus B)$.

Si tomamos ahora un elemento $z \in (C \setminus A) \cup (C \setminus B)$, observemos que z ha de estar, bien en $C \setminus A$, bien en $C \setminus B$, por lo que debe estar en C y *no estar* en A o en B. Así, $z \in C$, pero nunca puede estar en $A \cap B$, por lo que $z \in C \setminus (A \cap B)$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

1.6. Producto cartesiano. Relaciones de equivalencia.

Definición.– Dados dos conjuntos A y B, se define el *producto cartesiano* de A y B como el conjunto de pares ordenados formados (por este orden) por un elemento de A y uno de B y se denota

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}.$$

Dado $(a, b) \in A \times B$, el elemento $a \in A$ (respectivamente $b \in B$) se suele denominar primera (segunda) componente del par.

También se puede definir el producto cartesiano de una cantidad finita de conjuntos (para cantidades infinitas hay dos posibles generalizaciones y no las veremos aquí) de la forma natural

$$A_1 \times ... \times A_n = \prod_{i=1}^{n} A_i = \{(a_1, ..., a_n) \mid a_i \in A_i, \text{ para } i = 1, ..., n\}.$$

Definición.– Una *correspondencia* G de A en B es un subconjunto del producto $A \times B$. Equivalentemente se puede definir como una regla que asocia algunos elementos de A con algunos elementos de B. Concretamente, G asocia $a \in A$ con $b \in B$ si $(a, b) \in G$.

Definición.– Sea A un conjunto. Una *relación* R definida en A es una correspondencia de A en sí mismo.

Si el par $(x, y) \in A \times A$ está en R, diremos que x está R–relacionado con y, o relacionado con y por R. Esto se notará frecuentemente xRy (nótese que el orden es importante).

Definición.– Sea R una relación en A. Entonces diremos que R es:

(a) *Reflexiva* cuando para todo $x \in A$ se tiene que xRx.

(b) *Simétrica* cuando xRy implica yRx.

(c) *Antisimétrica* cuando xRy e yRx implican $x = y$ necesariamente.

(d) *Transitiva* cuando xRy e yRz implican xRz.

Las relaciones reflexivas, simétricas y transitivas se denominan *relaciones de equivalencia*. Las relaciones reflexivas, antisimétricas y transitivas se denominan *relaciones de orden*, pero no las trataremos aquí.

Ejemplos.– En el conjunto **Z** definimos las relaciónes siguientes:

$$xRy \iff x \leq y, \quad xSy \iff x - y \text{ es par}, \quad xTy \iff x \text{ divide a } y$$

Entonces R es una relación de orden (de hecho, las relaciones de orden se denominan así por ser éste el ejemplo fundamental) y S es una relación de equivalencia, mientras que T no es ninguna de ambas cosas. De hecho, notemos que S es de equivalencia si sustituimos la condición "$x - y$ es par" por la condición "$x - y$ es múltiplo de p", para cualquier número p que fijemos con antelación.

Definición.– Si R es una relación de equivalencia en A, denominamos *clase de equivalencia* de un elemento $x \in A$ al conjunto de todos los elementos de A relacionados con x, esto es,

$$\overline{x} = R(x) = \{y \in A \mid xRy\},$$

donde la primera notación se usa si R se sobreentiende, y la segunda si no es así.

Proposición.– Sea A un conjunto, R una relación de equivalencia en A. Entonces se verifican las siguientes propiedades:

(a) Todo elemento pertenece a una clase de equivalencia.

(b) Dos clases de equivalencia son disjuntas o iguales.

Esto es, la relación R divide completamente al conjunto A en subconjuntos disjuntos (las clases de equivalencia).

Demostración.– La afirmación (a) es trivial, ya que R es reflexiva. Para probar (b) supongamos que tenemos dos clases de equivalencia $R(x)$ y $R(y)$ de tal forma que existe $z \in R(x) \cap R(y)$. Tenemos que demostrar entonces que $R(x) = R(y)$, y lo haremos por doble inclusión. De hecho, sólo probaremos que $R(x) \subset R(y)$, porque la otra inclusión es absolutamente simétrica.

Tomamos entonces $a \in R(x)$. Como $z \in R(x)$, tenemos que aRx y xRz, por lo que aRz. De la misma forma, como $z \in R(y)$, se verifica que zRy. Así tenemos aRy, luego

$a \in R(y)$. Observemos que hemos usado tanto la propiedad simétrica como la transitiva para demostrar (b). $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Dada una relación de equivalencia R definida sobre un conjunto A, el conjunto cuyos elementos son las clases de equivalencia de A por R se denomina *conjunto cociente* de A por R. La notación ususal es

$$A/R = \{R(x) \mid x \in A\}.$$

Ejemplo.– Volviendo al ejemplo anterior, tomamos un entero p, fijado para lo que sigue, y consideramos

$$xSy \iff x - y \text{ es múltiplo de } p.$$

Entonces se tiene que, para todo $x \in \mathbf{Z}$

$$S(x) = \{y \in \mathbf{Z} \mid x \text{ e } y \text{ dan el mismo resto al dividirlos entre } p\},$$

por lo que

$$\mathbf{Z}/S = \{S(0), S(1), ..., S(p-1)\}.$$

1.7. Aplicaciones.

Definición.– Una *aplicación* f de A en B es una correspondencia donde todo elemento de A tiene asociado un único elemento de B. Esto es, en notación matemática, una correspondencia G es una aplicación si y sólo si se verifica que

$$\forall a \in A \quad \exists! b \in B \text{ tal que } (a, b) \in G.$$

Notación.– Es habitual denotar una aplicación entre conjuntos A y B de la forma $f : A \longrightarrow B$. En estas condiciones, dado $a \in A$ el único b verificando $(a, b) \in f$ se denota $f(a)$ y se denomina imagen de a (por f).

De esta notación surge la terminología, comúnmente usada, de llamar a A *conjunto original* (o dominio) y a B *conjunto imagen*.

En según qué contextos (por ejemplo, en Análisis Matemático, o cuando el conjunto de llegada es $\mathbf{R}^n$) es habitual llamar a las aplicaciones funciones, pero durante este curso utilizaremos la denominación aplicaciones.

Definición.– Dada una aplicación $f : X \longrightarrow Y$ y subconjuntos $A \subset X$ y $B \subset Y$, definimos:

(a) La *imagen* de A, notada $f(A)$, como

$$f(A) = \{y \in Y \mid \exists x \in A \text{ con } f(x) = y\} \subset Y,$$

esto es, el conjunto de elementos del conjunto imagen que son imagen de un elemento de A.

(b) La *anti–imagen* (o contraimagen, o imagen recíproca) de B, notada $f^{-1}(B)$, como

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

esto es, el conjunto de elementos del conjunto original cuya imagen está en B.

Proposición.– Sea $f : X \longrightarrow Y$ una aplicación, $A_1, A_2 \subset X$ y $B_1, B_2 \subset Y$. Se verifica:

(a) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$, $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.

(b) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

(c) $f(f^{-1}(B_1)) \subset B_1$, $A_1 \subset f^{-1}(f(A_1))$.

Demostración.– Vamos a probar, por ejemplo, la segunda afirmación de (a) y la primera de (c). Las demás son similares. Consideremos $y \in f(A_1 \cap A_2)$. Entonces existe $x \in A_1 \cap A_2$ tal que $y = f(x)$. Por tanto, $y \in f(A_1)$ e $y \in f(A_2)$, por lo que se tiene el resultado.

Es importante entender que, para afirmar que la otra inclusión no es cierta, basta con dar un contraejemplo; esto es, un caso particular donde no sea cierto el enunciado. Para ello consideremos $f : \mathbf{N} \longrightarrow \mathbf{N}$ definida por

$$f(x) = \begin{cases} x/2 + 1 & \text{si } x \text{ es par} \\ x + 2 & \text{si } x \text{ es impar} \end{cases}$$

Tomamos $A_1 = \{1, 3, 5\}$, $A_2 = \{2, 4, 6\}$. Claramente $f(A_1 \cap A_2) = f(\emptyset) = \emptyset$, pero $f(A_1) \cap f(A_2) = \{3\}$.

Probemos ahora que $f(f^{-1}(B_1)) \subset B_1$. Si $y \in f(f^{-1}(B_1))$, es porque existe $x \in f^{-1}(B_1)$ tal que $y = f(x)$. Pero, al ser $x \in f^{-1}(B_1)$, por definición tenemos que $y = f(x) \in B_1$.

Para demostrar que la inclusión contraria no es cierta en general podemos tomar la misma aplicación que en el caso anterior y considerar $B_1 = \{1, 3, 5\}$ nuevamente. Entonces $f^{-1}(B_1) = \{1, 3, 4, 8\}$ (por convenio, no incluimos el 0 en $\mathbf{N}$). Pero $f(f^{-1}(B_1)) = \{3, 5\}$, por lo que hemos acabado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Sea una aplicación $f : X \longrightarrow Y$.

(a) f se dice *inyectiva* si dos elementos distintos de X siempre tienen imágenes distintas. Dicho de otro modo, f es inyectiva si, de $f(x) = f(x')$, para $x, x' \in X$, se deduce que $x = x'$.

(b) f se dice *sobreyectiva (o sobre)* si todo elemento de Y es imagen de algún elemento de X. O sea, f es sobre si $f(X) = Y$.

(c) f se dice *biyectiva* si es inyectiva y sobreyectiva.

Observación.– Así, podemos decir que:

(a) f es inyectiva si y sólo si para todo $y \in Y$ $f^{-1}(\{y\})$ consta, a lo más, de un elemento.

(b) f es sobre si y sólo si para todo $y \in Y$ $f^{-1}(\{y\})$ consta, a lo menos, de un elemento.

(c) f es biyectiva si y sólo si para todo $y \in Y$ $f^{-1}(\{y\})$ consta, exactamente, de un elemento.

De esta forma, si f es biyectiva, existe una aplicación, denominada aplicación inversa y notada $f^{-1} : Y \longrightarrow X$, definida por $f^{-1}(y) = x$ si y sólo si $f(x) = y$.

Las aplicaciones inyectivas, sobres o biyectivas verifican algunas propiedades más concretas de las que enunciamos con anterioridad.

Definición.– Dadas dos aplicaciones $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ se define la *composición* de f y g, notada $g \circ f$, de X en Z como

$$(g \circ f)(x) = g(f(x)), \text{ para todo } x \in X.$$

Obviamente $g \circ f$ es una aplicación.

Observación.– Dadas aplicaciones entre conjuntos

$$X_1 \xrightarrow{f} X_2 \xrightarrow{g} X_3 \xrightarrow{h} X_4,$$

es elemental comprobar que $(h \circ g) \circ f = h \circ (g \circ f)$ (asociatividad de la composición de aplicaciones).

Definición.– Dada una aplicación $f : X \longrightarrow Y$ y un subconjunto $A \subset X$, se define la restricción de f a A como la aplicación

$$\begin{array}{rccc} f_{|A} : A & \longrightarrow & Y \\ x & \longmapsto & f_{|A}(x) = f(x) \end{array}$$

Esto es, $f_{|A}$ actúa exactamente como f, pero sólo sobre los elementos de A. Esto pone de manifiesto (o debería) lo importante que es, a la hora de definir una aplicación, determinar los conjuntos de partida y llegada, no sólo cómo se calcula la imagen de un elemento.

1.8. Estructuras. Grupos, anillos y cuerpos.

Definición.– Dado un conjunto G, una *operación interna binaria*, $\star$, en G es una aplicación

$$\begin{array}{rccc} \star : G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & \star(a, b) \end{array}$$

Habitualmente se utiliza la notación $\star(a, b) = a \star b$. Una *operación externa* (binaria) es exactamente lo mismo, salvo por el hecho de que el conjunto de partida es $X \times G$, para un cierto conjunto X distinto de G.

Un *grupo* es un par $(G, \star)$, compuesto por un conjunto G y una operación interna $\star$ en G, que verifica las siguientes propiedades:

(G.1) *Asociativa*: $a \star (b \star c) = (a \star b) \star c$, para cualesquiera $a, b, c \in G$.

(G.2) *Elemento neutro*: Existe un $e \in G$ tal que $a \star e = e \star a = a$, para todo $a \in G$.

(G.3) *Elemento opuesto*: Dado $a \in G$ existe $b \in G$ tal que $a \star b = b \star a = e$, el elemento neutro antes mencionado.

Si $(G, \star)$ posee además la propiedad conmutativa (esto es $a \star b = b \star a$ para cualesquiera $a, b \in G$), se dice que el grupo es abeliano o conmutativo.

Proposición.– Dado un grupo $(G, \star)$, el elemento neutro es único. Además, fijado $a \in G$, el elemento opuesto de a también es único.

Demostración.– Supongamos que e' es otro elemento neutro. Entonces

$$e = e \star e' = e' \star e = e'.$$

Sean ahora entonces b y c dos elementos opuestos de un $a \in G$ arbitrario, pero fijado en lo que sigue. Entonces

$$e = a \star b \implies c = c \star e = c \star a \star b = e \star b = b.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Notación.– Existen dos notaciones usuales para la operación en un grupo: la notación aditiva y la notación multiplicativa, que heredan las notaciones para los grupos conocidos $(k, +)$ y $(k \setminus \{0\}, \cdot)$, donde k puede ser $\mathbf{Q}$ o $\mathbf{R}$.

Si escribimos un grupo en notación aditiva, $(G, +)$, denotaremos 0 al elemento neutro y $-a$ al opuesto de a. Por el contrario, si usamos la notación multiplicativa, $(G, \cdot)$ denotaremos por 1 al elemento neutro y por a^{-1} o por $1/a$ al opuesto de a (que se denominará entonces inverso de a). Muchas veces la operación $\cdot$ se denota por simple yuxtaposición, esto es, ab en lugar de $a \cdot b$.

Observación.– Dado un grupo (pongamos en notación multiplicativa) G y un elemento $g \in G$ se puede probar (ejercicio fácil de doble inclusión) que el conjunto $g \cdot G = \{gx \mid x \in G\}$ es de nuevo G.

Definición.– Un *cuerpo* k es un conjunto con dos operaciones binarias internas, denominadas usualmente suma o adición $(+)$ y producto o multiplicación $(\cdot)$, de tal forma que

(C.1) $(k, +)$ es un grupo abeliano.

(C.2) $(k \setminus \{0\}, \cdot)$ es un grupo abeliano.

(C.3) Se da la propiedad distributiva de la suma respecto del producto:

$$a(b + c) = ab + ac, \quad \text{para cualesquiera } a, b, c, \in k.$$

Ejemplos.– Los ejemplos usuales de cuerpos son $\mathbf{Q}$ y $\mathbf{R}$. Veremos un ejemplo más adelante de gran impotancia: los números complejos.

En concreto el cuerpo $\mathbf{Q}$ podemos entenderlo como un buen ejemplo de relación de equivalencia. El conjunto base es, en este caso

$$X = \mathbf{Z} \times (\mathbf{Z} \setminus \{0\}) = \{\ (a,b) \mid a,b \in \mathbf{Z},\ b \neq 0\ \},$$

y la relación viene definida por

$$(a,b) \sim (a',b') \iff ab' = a'b.$$

En este contexto, la notación estándar para la clase de equivalencia del par (a,b) por la relación $\sim$ es, obviamente, a/b.

Definición.– Un *anillo* es un conjunto A dotado con dos operaciones binarias internas, usualmente denominadas suma o adición $(+)$ y producto o multiplicación $(\cdot)$, de tal forma que:

(A.1) $(A,+)$ es un grupo abeliano.

(A.2) La operación $(\cdot)$ es asociativa y posee elemento neutro (notado 1)[1].

(A.3) Se verifica la propiedad distributiva de la suma respecto del producto:

$$a \cdot (b+c) = a \cdot b + a \cdot c, \text{ para cualesquiera } a,b,c \in A.$$

Observación.– En un anillo A, $0 \cdot a = 0$ para todo $a \in A$, ya que

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

De similar forma se puede probar, por ejemplo, que $(-1) \cdot a = -a$ para todo $a \in A$.

Ejemplo.– El ejemplo fundamental de anillo son los enteros, $\mathbf{Z}$, con la suma y el producto usuales. Un ejemplo enormemente similar (luego veremos por qué) es el de los polinomios con coeficientes en $\mathbf{Q}$ o en $\mathbf{R}$.

1.9. Permutaciones (I): El grupo de las permutaciones.

Definición.– Consideremos el conjunto $A = \{1,2,...,n\}$ y sea

$$S_n = \{f : A \longrightarrow A \mid f \text{ biyectiva }\}.$$

El conjunto S_n se denomina conjunto de *permutaciones* de n elementos. Un cálculo elemental nos dice que S_n tiene exactamente $n!$ elementos.

Observación.– De la caracterización estudiada para las aplicaciones biyectivas se sigue que la composición de dos aplicaciones biyectivas es de nuevo biyectiva. Por tanto en S_n podemos definir una operación interna, que no es más que la composición de aplicaciones.

[1] Ésta es la definición más general posible de anillo, que admite la posibilidad de que el producto no sea abeliano, aunque en este curso los ejemplos que manejaremos serán casi todos *anillos abelianos* esto es, anillos donde el producto es conmutativo.

Esta operación verifica varias propiedades. Para empezar la aplicación, denominada identidad,

$$\begin{array}{rcl} \mathrm{Id} : A & \longrightarrow & A \\ i & \longmapsto & i \end{array}$$

verifica que, para todo $\sigma \in S_n$,

$$\sigma \circ \mathrm{Id} = \mathrm{Id} \circ \sigma = \sigma.$$

Por otra parte, dada $\sigma \in S_n$, se tiene que $\sigma^{-1} \in S_n$ también, y verifica

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{Id}.$$

Dado que la composición de aplicaciones es asociativa, hemos probado, pues, que $(S_n, \circ)$ es un grupo. De hecho, es un grupo *no* abeliano. Casi cualquier ejemplo no trivial de S_3 sirve para ver que, en general, si $\sigma, \tau \in S_n$, se tiene que $\sigma \circ \tau \neq \tau \circ \sigma$.

Notación.– Adoptaremos las siguientes notaciones indistintamente

$$\sigma \circ \tau = \sigma \cdot \tau = \sigma\tau$$

$$\sigma \circ ... \circ \sigma \ (r \text{ veces}) = \sigma^r$$

Observación.– Es posible entender cada aplicación de S_n como una reordenación del conjunto $\{1, ..., n\}$. De aquí es usual denotar los elementos de S_n como una tabla con dos filas: en la primera aparecen los números del 1 al n (para saber cuál es el conjunto original) y en la segunda aparece, bajo cada original, su imagen. Por ejemplo:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{bmatrix}$$

es la aplicación de $\{1, 2, 3, 4, 5\}$ en sí mismo que envía 1 en 4, 2 en 3, 3 en 2, 4 en 1 y 5 en sí mismo.

Vamos ahora a dar una cierta estructura al conjunto de las permutaciones. En primer lugar nos fijaremos en un tipo muy concreto (e interesante).

Definición.– Un *ciclo* de longitud r en S_n es una permutación σ tal que existen $\{a_1, ..., a_r\} \subset \{1, ..., n\}$, todos ellos distintos, verificando:

- $\sigma(a_j) = a_{j+1}$ para $j = 1, ..., r-1$, y $\sigma(a_r) = a_1$.
- $\sigma(i) = i$ para todo $i \notin \{a_1, ..., a_r\}$.

Esto es, los r elementos no fijos de σ pueden recorrerse todos yendo de original a imagen, empezando por uno cualquiera.

Los ciclos de longitud 2 se denominan trasposiciones.

Notación.– Un ciclo como el anterior se denotará, abreviadamente

$$\sigma = (a_1 \ ... \ a_r),$$

indicando con ello $\sigma(a_j) = a_{j+1}$ para $j = 1, ..., r-1$, y $\sigma(a_r) = a_1$.

Ejemplo.– El ejemplo visto anteriormente

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{bmatrix}$$

no es un ciclo. Hay cuatro elementos no fijos en σ y no pueden recorrerse yendo de original a imagen.

Observación.– La permutación inversa de un ciclo es un ciclo de la misma longitud. De hecho

$$(a_1\ a_2\ ...\ a_r)^{-1} = (a_r\ ...\ a_2\ a_1),$$

y, en particular, $(i\ j)^{-1} = (i\ j)$.

Observación.– Dos ciclos $\sigma = (a_1\ ...\ a_r)$ y $\tau = (b_1\ ...\ b_s)$ tales que

$$\{a_1, ..., a_r\} \cap \{b_1, ..., b_s\} = \emptyset$$

verifican que $\sigma \circ \tau = \tau \circ \sigma$. Estos ciclos se dicen disjuntos.

Proposición.– Toda permutación distinta de la identidad se puede descomponer en producto de ciclos disjuntos, de manera única (salvo reordenación de los ciclos).

Demostración.– Haremos la prueba por inducción en r, que será el número de elementos no fijos de σ. Si $r = 0$ no hay nada que probar, y $\sigma = \text{Id}$. Claramente r no puede ser 1, por la biyectividad de σ. Y, si $r = 2$, entonces llamamos $\{i, j\}$ a los elementos no fijos de σ y tenemos que tener, forzosamente

$$\sigma(i) = j,\ \sigma(j) = i \implies \sigma = (i\ j).$$

Sea $\sigma \in S_n$ dada por

$$\sigma = \begin{bmatrix} 1 & 2 & ... & n \\ a_1 & a_2 & ... & a_n \end{bmatrix}$$

y supongamos que tiene r elementos no fijos.

Comenzamos por el primer número i tal que $a_i \neq i$ y vamos creando la siguiente lista:

$$i \longmapsto \sigma(i) = a_i \longmapsto \sigma^2(i) \longmapsto \sigma^3(i) \longmapsto ...$$

Dado que $\sigma \in S_n$, existirán $s, t \in \mathbf{N}$ (pongamos $s < t$) tal que

$$\sigma^s(i) = \sigma^t(i)$$

y, componiendo con $(\sigma^{-1})^s$ obtenemos

$$i = \sigma^{t-s}(i).$$

Sea r el menor entero positivo tal que $i = \sigma^r(i)$. Entonces el ciclo de longitud r

$$(i\ \sigma(i)\ ...\ \sigma^{r-1}(i))$$

actúa, por construcción, de la misma forma que σ sobre el conjunto $\{i, \sigma(i), ..., \sigma^{r-1}(i)\}$.

Sólo resta aplicar el mismo razonamiento (hipótesis de inducción) a la permutación τ, definida por

$$\tau(j) = \begin{cases} \sigma(j) & \text{si } j \notin \{i, \sigma(i), ..., \sigma^{r-1}(i)\} \\ j & \text{si } j \in \{i, \sigma(i), ..., \sigma^{r-1}(i)\} \end{cases}$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Ejemplo.– En el ejemplo anterior

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{bmatrix} = (1\ 4)\,(2\ 3).$$

Observación.– Si admitimos ciclos de longitud 1 (con la definición obvia) podemos obtener una descripción más precisa de la permutación. En efecto,

$$(1\ 4)\,(2\ 3)$$

puede ser la permutación del ejemplo anterior. Pero también puede ser

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 5 & 6 \end{bmatrix} \in S_6.$$

Si queremos evitar estas confusiones, escribiremos el ejemplo del principio como

$$(1\ 4)\,(2\ 3)\,(5).$$

1.10. Permutaciones (II): Trasposiciones.

Definición.– Llamaremos *orden* de una permutación σ, notado $o(\sigma)$, al menor entero r tal que $\sigma^r = \text{Id}$.

Observación.– Notemos que el orden de una permutación siempre está bien definido. Dado que S_n tiene $n!$ elementos, el conjunto $\{\sigma^i \mid i \in \mathbf{N}\}$ debe contener elementos repetidos. Y entonces, si $\sigma^s = \sigma^t$ (con $s < t$), es sencillo comprobar que $\sigma^{t-s} = \text{Id}$.

Observación.– Sea σ una permutación de orden r. Si t es tal que $\sigma^t = \text{Id}$, entonces $r|t$.

Podemos hallar fácilmente el orden de una permutación a partir de su descomposición en ciclos disjuntos.

Proposición.– Sea $\sigma \in S_n$, con descomposición en ciclos disjuntos dada por

$$\sigma = C_1 \cdot C_2 \cdot ... \cdot C_r,$$

donde la longitud de C_i es, pongamos l_i. Entonces

$$o(\sigma) = \text{mcm}(l_1, ..., l_r).$$

Demostración.– Probemos primero que, si C es un ciclo de longitud l, $o(C) = l$. Esto es muy sencillo, dado que, si j es un elemento no fijo por C, es evidente por la definición de ciclo que

$$C^l(j) = j, \quad C^s(j) \neq j \text{ para } s < l.$$

Como los elementos fijos por C lo son también por C^l, se tiene que $C^l = \text{Id}$, y $C^s \neq \text{Id}$ para cualquier $s < l$.

Ahora pasamos al caso general. Dado que al componer ciclos disjuntos es irrelevante el orden tenemos que, para todo $s \in \mathbf{N}$

$$\sigma^s = C_1^s \cdot C_2^s \cdot ... \cdot C_r^s.$$

Como los C_i actúan de forma no trivial sobre elementos distintos de $\{1, ..., n\}$, para que $\sigma^s = \text{Id}$ tiene que ser $C_i^s = \text{Id}$ para $i = 1, ..., s$. Así pues el orden de σ será el menor múltiplo común de los órdenes de los C_i. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Aparte de la factorización en ciclos disjuntos, podemos dar otro tipo de descomposición para las permutaciones de S_n. Reducimos los elementos necesarios, a cambio de perder propiedades, como la unicidad.

Proposición.– Toda permutación se puede descomponer en producto de trasposiciones.

Demostración.– Esta demostración es mucho más simple, dado que basta probarlo para un ciclo, y esto es muy sencillo. Sólo hay que comprobar

$$(a_1\ a_2\ ...\ a_r) = (a_1\ a_r) ... (a_1\ a_3)\,(a_1\ a_2).$$

Observación.– La descomposición anterior, sin embargo, no es única. Por ejemplo,

$$(1\ 2\ 3) = (1\ 3)\,(1\ 2) = (3\ 2)\,(1\ 3).$$

Sin embargo, no es casual el hecho de que ambas descomposiciones consten de dos trasposiciones.

Proposición.– Sea $\sigma \in S_n$ una permutación. Entonces todas las posibles descomposiciones de σ como producto de trasposiciones consta de, bien un número par, bien un número impar de factores.

Demostración.– La demostración es interesante porque sigue un camino indirecto: en lugar de trabajar con las permutaciones como objetos en sí, usaremos cómo las permutaciones actúan sobre otro objeto, en este caso un polinomio en n variables.

Consideremos el polinomio

$$F(x_1, ..., x_n) = \prod_{i<j} (x_i - x_j) = (x_1 - x_2) \cdot ... \cdot (x_1 - x_n) \cdot (x_2 - x_3) \cdot ... \cdot (x_{n-1} - x_n).$$

Entonces hacemos actuar σ sobre F de la siguiente manera

$$\sigma(F) = F\left(x_{\sigma(1)}, ..., x_{\sigma(n)}\right),$$

es decir, renombramos las variables en F siguiendo a σ. Del mismo modo tenemos

$$\sigma(F) = \prod_{i<j} \left(x_{\sigma(i)} - x_{\sigma(j)}\right).$$

Ahora bien, notemos que una trasposición $(r\ s)$ (pongamos con $r < s$) verifica que

$$(r\ s)(F) = -F.$$

Veamos esto en la descomposición de F en factores $(x_i - x_j)$:

- Si $\{r,s\} \cap \{i,j\} = \emptyset$, entonces $(x_i - x_j)$ no se ve afectado por $(r\ s)$.
- Si $i < r < s = j$, entonces $(x_i - x_j)$ va en $(x_i - x_r)$ y $(x_i - x_r)$ va en $(x_i - x_s) = (x_i - x_j)$.
- Si $r < i < s = j$, entonces $(x_i - x_j)$ va en $(x_i - x_r)$ y $(x_r - x_i)$ va en $(x_s - x_i) = (x_j - x_i)$, con lo cual el producto de ambos factores permanece inalterado por la acción de $(r\ s)$.
- Si $r < s = i < j$, entonces $(x_j - x_i)$ va en $(x_r - x_i)$ y $(x_r - x_i)$ va en $(x_s - x_i) = (x_j - x_i)$.
- Por último $(r\ s)(x_r - x_s) = -(x_r - x_s)$.

Por tanto, cada trasposición cambia de signo F al actuar sobre él. Así σ, al ser producto de trasposiciones, puede dejar F invariante o cambiarlo de signo, dependiendo de si σ se escribe como producto de una cantidad par o impar de trasposiciones, respectivamente. Pero la acción de σ sobre F es independiente de cómo se escriba σ como producto de trasposiciones, luego la cantidad de factores ha de ser siempre par o siempre impar. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

1.11. Permutaciones (III): Paridad.

Observación.– Una cierta forma de medir cuánto altera una permutación $\sigma \in S_n$ el orden natural en $\{1,2,...,n\}$ es ver el número de inversiones que σ efectúa: para cada $i \in \{1,2,...,n\}$ se cuenta una inversión por cada $j > i$ tal que $\sigma(i) > \sigma(j)$. En nuestro ejemplo anterior

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{bmatrix} = (1\ 4)\,(2\ 3).$$

tenemos que contar:

- Tres inversiones porque $\sigma(1) > \sigma(2), \sigma(3), \sigma(4)$.
- Dos inversiones porque $\sigma(2) > \sigma(3), \sigma(4)$.
- Una inversión porque $\sigma(3) > \sigma(4)$.

Luego el número de inversiones de σ es 6. Este concepto será útil para la definición de determinante, pero además está íntimamente ligado a la descomposición en producto de trasposiciones.

Observación.– El número de inversiones también puede contarse al revés: esto es, contar una inversión por cada $j > i$ tal que $\sigma(i) > \sigma(j)$.

Observación.– Una forma sencilla de contar el número de inversiones de una permutación σ es dibujar la aplicación usando diagramas de Venn y trazando flechas que vayan de i a $\sigma(i)$. Entonces, si hemos dispuesto $1,...,n$ de forma ordenada en ambos diagramas de Venn, el número de trasposiciones de σ es el número de cruces que se producen entre las flechas.

Proposición.– Sea $\sigma \in S_n$ una permutación con k inversiones. Entonces existe una descomposición de σ en producto de k trasposiciones.

Demostración.– Supongamos que tenemos

$$\sigma = \begin{bmatrix} 1 & 2 & ... & n \\ a_1 & a_2 & ... & a_n \end{bmatrix},$$

y supongamos que $a_1 = r \neq 1$. Esto quiere decir que 1 aporta $r-1$ inversiones, dado que los elementos $1, ..., r-1$, menores que r verificarán que sus anti–imágenes, pongamos $x_1 < ... < x_{r-1}$ son mayores que la de r, que es 1.

Entonces podemos darnos cuenta de que

$$(r\ \sigma(x_{r-1}))\ ...\ (r\ \sigma(x_1))\sigma$$

es una permutación, cuya diferencia con r consiste en que hemos *movido* r hasta situarlo como imagen de r, para lo cual hemos usado $r-1$ trasposiciones, exactamente el número de inversiones que aporta 1 (o el que aporta r si las contamos al revés). Repitiendo el proceso con la imagen de 2 (y sucesivamente) llegamos a una expresión de la forma

$$\tau_1 \cdot ... \tau_k \cdot \sigma = \mathrm{Id},$$

donde recordemos que k es el número de inversiones de σ. De aquí se deduce fácilmente que

$$\sigma = \tau_1^{-1} \cdot ... \cdot \tau_k^{-1} = \tau_1 \cdot ... \cdot \tau_k,$$

como queríamos. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

1.12. El cuerpo de los números complejos.

Definición.– Un *número complejo* es un número de la forma $a + b \cdot i$, donde a y b son números reales e i es un símbolo que verifica la propiedad $i^2 = -1$.

Dado un complejo $z = a + b\,i$, el número real a se denomina parte real de z, notado $\Re(z)$, mientras que b se denomina parte imaginaria de z, notado $\Im(z)$.

Dotamos a $\mathbf{C}$ de una estructura de cuerpo con las siguientes operaciones:

$$(a + b\,i) + (c + d\,i) = (a + c) + (b + d)\,i,$$

$$(a + b\,i)(c + d\,i) = (ac - bd) + (ad + bc)\,i,$$

regla esta última que puede ser fácilmente recordada si decimos que i representa $\sqrt{-1}$.

Comprobar que $\mathbf{C}$ con estas dos operaciones es un cuerpo es algo tedioso. Simplemente notaremos que el elemento neutro de la suma es $0 = 0 + 0\,i$ y el neutro del producto es $1 = 1 + 0\,i$. Así mismo, dado $a + b\,i$ el inverso aditivo es $-a + (-b)\,i$ y, si es distinto de 0, el inverso multiplicativo es precisamente $a/(a^2 + b^2) - (b/(a^2 + b^2))\,i$.

Observación.– Algunas propiedades interesantes de los número complejos son las siguientes:

(a) Si consideramos los números complejos de la forma $a + 0\,i$ veremos que podemos suponer $\mathbf{R} \subset \mathbf{C}$, identificando $a \in \mathbf{R}$ con $a + 0\,i \in \mathbf{C}$.

(b) Dado un complejo $z = a+b\,i$, el complejo $\overline{z} = a-b\,i$ se denomina su conjugado. La operación de conjugación, a pesar de su inofensivo aspecto, tiene una importancia enorme, incluso en el estudio de objetos reales. Un par de propiedades inmediatas, a partir de la definición, son las siguientes:

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \qquad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2},$$

de donde a su vez se deducen

$$\overline{-z} = -\overline{z}, \qquad \overline{1/z} = 1/\overline{z}.$$

(c) El producto

$$z \cdot \overline{z} = a^2 + b^2$$

es un real positivo, y su raíz cuadrada se llama el módulo de z, denotado $|z|$. De hecho, la expresión del inverso multiplicativo de z resulta más sencilla usando $\overline{z}$:

$$\frac{1}{z} = \frac{\overline{z}}{\overline{z}} \cdot \frac{1}{z} = \frac{\overline{z}}{|z|}.$$

(d) Todo número complejo z se puede escribir de forma

$$z = |z|(a + b\,i),$$

donde $a^2 + b^2 = 1$ y, en consecuencia, existe un único ángulo $\alpha \in [0, 2\pi)$, llamado argumento de z, tal que

$$z = |z|(\cos(\alpha) + \text{sen}(\alpha)\,i).$$

Con esta notación es fácil ver que para multiplicar dos números complejos hay que multiplicar sus módulos y sumar sus argumentos. Para dividir, por tanto, se dividen sus módulos y se restan sus argumentos. En efecto: sean

$$z_1 = r_1(\text{cos}(\alpha_1) + i\text{sen}(\alpha_1)), \qquad z_2 = r_2(\text{cos}(\alpha_2) + i\text{sen}(\alpha_2)).$$

Entonces

$$\begin{aligned} z_1 z_2 &= r_1 r_2 \cdot [(\text{cos}(\alpha_1) + i\text{sen}(\alpha_1))(\text{cos}(\alpha_2) + i\text{sen}(\alpha_2)] \\ &= r_1 r_2 \cdot [\,(\text{cos}(\alpha_1)\text{cos}(\alpha_2) - \text{sen}(\alpha_1)\text{sen}(\alpha_2)) + \\ &\qquad (\text{cos}(\alpha_1)\text{sen}(\alpha_2) + \text{cos}(\alpha_2)\text{sen}(\alpha_1))\,i\,] \\ &= r_1 r_2 \cdot [\text{cos}(\alpha_1 + \alpha_2) + i\text{sen}(\alpha_1 + \alpha_2)]\,. \end{aligned}$$

De aquí se obtiene la fórmula de De Moivre:

Teorema.– Para todo número natural n, se tiene

$$(\text{cos}(\alpha) + i\text{sen}(\alpha))^n = \text{cos}(n\alpha) + i\text{sen}(n\alpha).$$

Demostración.– Lo probaremos por inducción. Para $n = 0$ se verifica, pues

$$(\cos(\alpha) + i\text{sen}(\alpha))^0 = 1 = \cos(0) + i\text{sen}(0).$$

Supongamos que se verifica para n, es decir,

$$(\cos(\alpha) + i\text{sen}(\alpha))^n = \cos(n\alpha) + i\text{sen}(n\alpha).$$

Entonces,

$$(\cos(\alpha) + i\text{sen}(\alpha))^{n+1} = (\cos(\alpha) + i\text{sen}(\alpha))^n(\cos(\alpha) + i\text{sen}(\alpha)) =$$

$$= (\cos(n\alpha) + i\text{sen}(n\alpha)(\cos(\alpha) + i\text{sen}(\alpha)) = \cos(n+1)\alpha + i\text{sen}(n+1)\alpha.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Tema 2. El anillo de los números enteros.

2.1. Divisibilidad.

Antes de comenzar el tema enunciamos una propiedad de los números enteros que usaremos más adelante:

Principio de la buena ordenación: Todo subconjunto no vacío de $\mathbf{Z}$ acotado inferiormente posee un mínimo.

Desarrollamos brevemente la teoría clásica de la divisibilidad sobre los números enteros.

Definición.- Sean a, b dos enteros distintos de cero. Se dirá que a *divide a* b si existe $c \in \mathbf{Z}$ tal que $ac = b$. En este caso se escribe $a|b$. También se dice que b es *divisible* por a.

Observación.– Dos elementos especiales de $\mathbf{Z}$ son 1 y -1. Para empezar, obviamente dividen a todos los números enteros. Pero además son los únicos enteros con esta propiedad.

Supongamos que $a \in \mathbf{Z}$ es otro entero con esta propiedad. Entonces debe dividir a 1, luego existe b tal que $ab = 1$. Entonces, o bien a, b son positivos o son negativos. Si son negativos, se pone $(-a)(-b) = 1$, con lo que se puede suponer que ambos son positivos.

En este caso, si fuese a ó b mayor que 1 (por ejemplo a), sería $a > 1$ y $b > 0$ (luego $b \geq 1$) sería $ab > 1 \cdot b = b \geq 1$, luego $ab > 1$, lo que no puede ser. Así, $a = b = 1$, luego desde el principio $a = \pm 1$, $b = \pm 1$.

Observación.– La relación de divisibilidad verifica las propiedades siguientes:

1. Propiedad reflexiva: $a|a$. En efecto, $a = 1 \cdot a$.

2. Propiedad antisimétrica: $a|b$ y $b|a$ implican que $a = \pm b$. En efecto, existen c, c' tales que $b = ac$ y $a = bc'$. Así $a = acc'$, luego $a - acc' = a(1 - cc') = 0$. Como $a \neq 0$ por definición de divisibilidad, es $1 - cc' = 0$ luego $cc' = 1$, de donde $c' = \pm 1$ y así $a = \pm b$.

3. Propiedad transitiva: Si $a|b$ y $b|c$ entonces $a|c$. En efecto, existen d, d' tales que $b = ad$ y $c = bd'$, luego $c = add'$ lo que implica que $a|c$.

Por consiguiente, si nos restringimos a enteros positivos, la divisibilidad es una relación de orden parcial porque la propiedad antisimétrica se enuncia así: $a|b$ y $b|a \Longrightarrow a = b$.

Observación.– La divisibilidad es compatible con las operaciones aritméticas. En concreto:

1. Si $a|b$ y $a|c$ entonces $a|(b \pm c)$. En efecto, existen $d, d' \in \mathbf{Z}$ tales que $b = ad$ y $c = ad'$. Así
$$b \pm c = ad \pm ad' = a(d \pm d')\,,$$
luego $a|(b \pm c)$.
2. Si $a|b$ entonces $a|bc$, $\forall c \in \mathbf{Z}$. En efecto, existe $d \in \mathbf{Z}$ tal que $b = ad$. Así $bc = adc$, luego $a|bc$.

Veamos ahora uno de los resultados más importantes de este tema:

Teorema (de la división euclídea).– Sean $a, b \in \mathbf{Z}_+$, $b > 0$; Existen unos enteros únicos $q, r \in \mathbf{Z}$ tales que:

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

Al entero q se le llama el *cociente* de la división y a r el *resto*.

Demostración.– Vamos a probar primero la existencia. Si $a < b$, entonces se puede poner $q = 0$ y $r = a$. Supongamos que $a \geq b$ y sea $q \in \mathbf{Z}$ tal que $qb \leq a < (q+1)b$. Pongamos $r = a - bq$; hay que demostrar que $0 \leq r < b$. Desde luego, como $a \geq qb$ es $a - qb = r \geq 0$. Por otro lado, como $a < (q+1)b$, se tiene que $r = a - qb < (q+1)b - qb = b$.

Probemos ahora la unicidad. Supongamos que existen $q', r' \in \mathbf{Z}$ tales que $a = q'b + r', 0 \leq r < b$. Si $q \geq q'$, restando obtenemos que $(q - q')b = r' - r < b$, igualdad que sólo se puede dar si $q = q'$ y $r = r'$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Este teorema se puede demostrar usando el principio de buena ordenación. En efecto: sea $S = \{a - bx \quad | \quad x \in \mathbf{Z} \text{ y } a - bx \geq 0\}$. S es no vacío y está acotado inferiormente, luego posee un mínimo. Sea $r = a - bq \geq 0$ dicho mínimo. Falta ver que $r < b$. En caso contrario, $r = b + r'$, $0 \leq r' < r$. Sustituyendo se tiene que $r' = a - b(q+1) \in S$, en contra de ser r el mínimo.

Observación.– Podemos dar una nueva definición de divisibilidad: Sean a, b dos enteros distintos de cero. Se dirá que b divide a a si el resto de la división de a por b es cero.

Definición.– Un entero $p \neq 0, \pm 1$ se llama *primo* si y sólo si es divisible únicamente por $\pm p$ y ± 1.

Definición.– Dados dos enteros a, b, diremos que $d > 0$ es *un máximo común divisor* de a y b y denotaremos $d = \text{mcd}(a, b)$, si se verifica:

1. $d|a$ y $d|b$.
2. Si $d' > 0$ es tal que $d'|a$ y $d'|b$ entonces $d'|d$.

Si $d = 1$ se dice que a y b son *primos entre sí*.

Diremos que $m > 0$ es un *mínimo común múltiplo* de a y b y denotaremos $m = \text{mcm}(a, b)$, si se verifica:

1. $a|m$ y $b|m$.
2. Si $m' > 0$ es tal que $a|m'$ y $b|m'$ entonces $m|m'$.

Observación.– Por el momento no tenemos asegurada la existencia del mcd ni del mcm de dos enteros, pero es fácil comprobar que, de existir, son únicos.

Veamos el caso del mcd. Supongamos que d y f son dos mcd de a y b. Por ser d un mcd y verificarse que $f|a, f|b$, por la propiedad 2) se tiene que $f|d$. Cambiando el papel de d y f, tenemos $d|f$, y por tanto la igualdad.

2.2. Algoritmo de Euclides. Identidad de Bezout.

Veamos un procedimiento, el algoritmo de Euclides, para el cálculo del máximo común divisor.

Proposición.– Sean $a, b \in \mathbf{Z}_+$, $a \geq b$, y efectuemos la división euclídea $a = qb + r$. Entonces, si $r = 0$ es $\text{mcd}(a, b) = b$ y si $r \neq 0$

$$\text{mcd}(a, b) = \text{mcd}(b, r).$$

Demostración.– Si $r = 0$ es $a = qb$, luego $\text{mcd}(a, b) = b$. Si $r \neq 0$, sea

$$d = \text{mcd}(a, b), \quad d' = \text{mcd}(b, r)\ ;$$

entonces $d|r = a - qb$, luego $d|d'$. Por otra parte, $d'|a = qb + r$, luego $d'|d$ y así $d = d'$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Este resultado nos permite describir el **Algoritmo de Euclides:** Sean $a, b \in \mathbf{Z}_+$, $a \geq b$, y efectuemos la división euclídea $a = qb + r$. Como $r < b$, podemos dividir b entre r, y así sucesivamente, obteniendo:

$$\begin{array}{lcll} a & = & qb + r & 0 \leq r < b \\ b & = & q_0 r + r_1 & 0 \leq r_1 < r \\ r & = & q_1 r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = & q_2 r_2 + r_3 & 0 \leq r_3 < r_2 \\ & \vdots & & \\ r_{n-1} & = & q_n r_n + r_{n+1} & 0 \leq r_{n+1} < r_n \\ r_n & = & q_{n+1} r_{n+1} + 0 & r_{n+2} = 0 \end{array}$$

Proposición.– Se tiene que $\text{mcd}(a, b) = r_{n+1}$, es decir, el máximo común divisor de a y b es el último resto no nulo al aplicar sucesivamente el algoritmo de división.

Demostración.– Por la proposición anterior se tiene que:

$$\text{mcd}(a, b) = \text{mcd}(b, r) = \text{mcd}(r, r_1) = \ldots = \text{mcd}(r_{n-1}, r_n) = \text{mcd}(r_n, r_{n+1}) = r_{n+1},$$

lo cual demuestra el resultado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Asociada al máximo común divisor está la identidad de Bézout, cuya existencia teórica viene afirmada por el siguiente teorema:

Teorema (Identidad de Bézout).– Sean $a, b > 0$ enteros y sea $d = \text{mcd}(a, b)$. Existen enteros α, β tales que

$$\alpha a + \beta b = d$$

A cualquier igualdad de este tipo se le llama *identidad de Bézout*.

Demostración.– Demostramos la existencia de manera no constructiva. Sea

$$S = \{n \in \mathbf{Z}_+ \mid n = xa + yb,\ x, y \in \mathbf{Z}\}\,;$$

evidentemente $S \neq \emptyset$ porque $a = 1 \cdot a + 0 \cdot b \in S$. Como S está acotado inferiormente por cero, tiene un mínimo al que llamamos $n_0 = \alpha a + \beta b$. Como $d|a$ y $d|b$ entonces $d|n_0$. Vamos a probar que $d = n_0$, para lo que hay que demostrar que $n_0|a$ y $n_0|b$. Vamos a probar que $n_0|a$, la otra relación se prueba de forma análoga. Por la división euclídea podemos escribir $a = qn_0 + r$ con $0 \leq r < n_0$. Entonces,

$$r = a - qn_0 = a - q(\alpha a + \beta b) = (1 - q\alpha)a + (-q\beta)b \in S\,.$$

Por la minimalidad de n_0 tiene que ser $r = 0$, luego $n_0|a$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Los enteros α y β que aparecen en la identidad de Bézout no son únicos. En efecto: para cualesquiera α, β tales que $\alpha a + \beta b = d$, es

$$(\alpha - kb)a + (\beta + ka)b = d, \quad \forall k \in \mathbf{Z}\,.$$

La identidad de Bézout nos permite probar el siguiente teorema:

Teorema de Euclides.– Sean $a, b, c > 0$ tales que $c|ab$ y $\text{mcd}(c, a) = 1$; entonces $c|b$. En particular, si p es primo, $p|ab$ y p no divide a a, entonces $p|b$.

Demostración.– Evidentemente, la segunda afirmación es consecuencia de la primera; demostremos ésta. Por la identidad de Bézout, $1 = \alpha a + \beta c$. Multiplicando por b esta expresión, se tiene que $b = \alpha ab + \beta cb$. Como $c|ab$ y $c|cb$, $c|b$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Sea

$$d = \text{mcd}(a, b), \quad , a' = \frac{a}{d}, \quad b' = \frac{b}{d}\,.$$

Entonces a', b' son primos entre sí porque si no, y $1 \neq d'|a'$ y $d'|b'$, sería $d < dd'|a$, $dd'|b$, lo que no es posible.

Ahora podemos definir el mínimo común múltiplo usando el máximo común divisor. Sean $a, b \in \mathbf{Z}$, $d = \text{mcd}(a, b)$.

Proposición.– Se verifica que $\text{mcm}(a, b) = ab/d$.

Demostración.– Sean

$$m = ab/d, \quad a' = a/d, \quad b' = b/d.$$

Se tiene que $m = a'b = ab'$, luego es múltiplo de a y b. Sea $m' \in \mathbf{Z}$ múltiplo de a y b, $m' = aa'' = bb''$. Dividiendo esta última igualdad por d obtenemos $a'a'' = b'b''$ y, por el

teorema de Euclides, $a'|b''$, es decir, $b'' = a'c$. Sustituyendo $m' = ba'c = mc$, luego m es el mínimo común múltiplo de a y b. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Teorema (fundamental de la divisibilidad).– Todo entero distinto de 0 y ± 1 se descompone en producto finito de números primos. Esta descomposición es única salvo orden y producto por unidades.

Demostración.– Vamos primero a demostrar la existencia de la descomposición. Sea $n \neq 0, \pm 1$ un entero fijo, y vamos a demostrar que n se descompone en producto de primos. Podemos suponer que $n > 0$ porque, si lo demostramos en este caso y $n = p_1 \cdots p_r$, entonces $-n = (-p_1) \cdots p_r$, lo que demuestra el resultado para los enteros negativos.

La existencia de la descomposición se prueba por inducción a partir de $n = 2$. El número $n = 2$ es primo. Supongamos que $n > 2$ y que todos los números menores que n se descomponen en producto finito de primos. Si n es primo hemos terminado: es producto de un primo (él mismo). Si no lo es, se descompone en producto $n = n_1 n_2$ de dos enteros positivos estrictamente menores que n. Al aplicar a n_1 y n_2 la hipótesis de inducción, vemos que n se descompone en producto finito de primos.

Para demostrar la unicidad (salvo orden y producto por unidades), basta considerar enteros positivos n por la misma razón que antes. Además, basta ver que no puede haber dos descomposiciones distintas de un mismo número positivo en producto de primos positivos. Vamos a operar por reducción al absurdo. Supongamos que hay números que admiten dos descomposiciones distintas en producto de primos positivos:

$$n = p_1 \cdots p_r = q_1 \cdots q_s.$$

Supongamos que $r \leq s$. Tenemos $p_1 | n = q_1 \cdots q_s$, luego $p_1 | q_i$, para algún i, con $1 \leq i \leq s$, de donde $p_1 = q_i$, al ser q_i primo. Podemos suponer $i = 1$. Dividiendo por p_1 se tiene que $p_2 \cdots p_r = q_2 \cdots q_s$. Repitiendo el razonamiento para $p_2, \ldots, p_r$, llegamos a $1 = q_{r+1} \cdots q_s$. Luego $r = s$ y $p_i = q_i, \quad i = 1, \ldots, r$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Teorema (Euclides).– El conjunto de los primos es infinito.

Demostración.– Supongamos que no, es decir, que el conjunto de los primos fuese finito, y sean $p_1, \ldots, p_r$ todos los primos. Sea $n = p_1 \cdots p_r + 1$. Por la factorización única, n debe ser divisible por algún p_i, lo que implicaría que $p_i | 1$ y eso es imposible. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Veamos otra forma de definir el máximo común divisor y el mínimo común múltiplo. La factorización única de un entero positivo n la escribiremos usualmente en la forma

$$n = \prod_{p \text{ primo}} p^{\nu_n(p)}$$

donde todos los $\nu_n(p)$ son cero salvo un número finito. La factorización se puede extender a enteros $n < 0$ poniendo

$$n = (-1) \prod_{p \text{ primo}} p^{\nu_{-n}(p)}.$$

Sin embargo, la noción de número primo la reservaremos para los positivos, como hemos dicho antes.

Teorema (Existencia del máximo común divisor).– Dados dos enteros $a, b > 0$, existe un único $d > 0$ que verifica:

1. $d|a$ y $d|b$.
2. Si $d' > 0$ es tal que $d'|a$ y $d'|b$ entonces $d'|d$.

A este entero se le llama el máximo común divisor de a y b y se le denota $d = \text{mcd}(a, b)$.

Demostración.– Sean

$$a = \prod_{p \text{ primo}} p^{\nu_a(p)}, \quad b = \prod_{p \text{ primo}} p^{\nu_b(p)}$$

las descomposiciones de a y b en producto de primos. Según el enunciado queda claro que el único número que satisface las condiciones es

$$d = \prod_{p \text{ primo}} p^{\min(\nu_a(p),\nu_b(p))}.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Teorema (Existencia del mínimo común múltiplo).– Dados dos números $a, b > 1$, existe un único $m > 0$ que verifica:

1. $a|m$ y $b|m$.
2. Si $m' > 0$ es tal que $a|m'$ y $b|m'$ entonces $m|m'$.

A este entero se le llama el mínimo común múltiplo de a y b y se le denota $m = \text{mcm}(a, b)$.

Demostración.– Sean

$$a = \prod_{p \text{ primo}} p^{\nu_a(p)}, \quad b = \prod_{p \text{ primo}} p^{\nu_b(p)}$$

las descomposiciones de a y b en producto de primos. Según el enunciado queda claro que el único número que satisface las condiciones es

$$m = \prod_{p \text{ primo}} p^{\max(\nu_a(p),\nu_b(p))} = \frac{ab}{\text{mcd}(a, b)}$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

2.3. Congruencias.

La división euclídea nos conduce inmediatamente a la noción de congruencia de módulo dado.

Definición.– Dados dos enteros a, b, se dirá que a *es congruente con* b *módulo* $m \neq 0$ si a y b dan el mismo resto en la división euclídea por m. En este caso se escribirá $a \equiv b \pmod m$.

De la división euclídea se deduce que siempre se puede suponer positivo el módulo m de la congruencia porque $a = qm + r$ implica $a = (-q)(-m) + r$. Esto es lo que haremos de ahora en adelante.

Se puede ver a las congruencias de módulo $m > 0$ fijo como una relación en $\mathbf{Z}$. En este sentido es una relación de equivalencia porque verifica las siguientes propiedades (que son consecuencia inmediata de la definición):

1. Propiedad reflexiva: Para todo $a \in \mathbf{Z}$ es $a \equiv a \pmod{m}$.
2. Propiedad simétrica: Si $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$.
3. Propiedad transitiva: Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$.

Una propiedad fundamental de las congruencias es la siguiente:

Proposición.– $a \equiv b \pmod{m}$ si y sólo si $m|(b-a)$.

Demostración.– En efecto, si $a \equiv b \pmod{m}$, entonces $a = qm + r$, $b = q'm + r$, luego $b - a = (q' - q)m$. Recíprocamente, si $m|(b-a)$, $a = qm + r$ $b = q'm + r'$, entonces $b - a = (q' - q)m + (r' - r)$, igualdad que sólo es posible cuando $r' - r = 0$ ya que $|r' - r| < m$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Las congruencias son compatibles con la adición y la multiplicación.

Proposición.– Se verifica que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m} \Longrightarrow a + c \equiv b + d \pmod{m}$.

Demostración.– En efecto, considerando las divisiones euclídeas

$$\begin{array}{rr} a = q_1m + r_1 & b = q_2m + r_1 \\ c = q_3m + r_2 & d = q_4m + r_2 \end{array}$$
$$r_1 + r_2 = q_5m + r_3$$
$$a + c = (q_1 + q_3 + q_5)m + r_3 \quad b + d = (q_2 + q_4 + q_5)m + r_3$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Proposición.– Se verifica que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m} \Longrightarrow ac \equiv bd \pmod{m}$.

Demostración.– En efecto, considerando las divisiones euclídeas

$$\begin{array}{rr} a = q_1m + r_1 & b = q_2m + r_1 \\ c = q_3m + r_2 & d = q_4m + r_2 \end{array}$$
$$r_1r_2 = q_5m + r_3$$
$$ac = (q_1q_3m + q_1r_2 + q_3r_1 + q_5)m + r_3$$
$$bd = (q_2q_4m + q_2r_2 + q_4r_1 + q_5)m + r_3$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Las congruencias tienen algunas propiedades interesantes que las diferencian de los enteros. ¿Qué ocurre con la cancelación multiplicativa de congruencias? Es decir, se trata de ver si se verifica que

$$ax \equiv bx \pmod{m} \Longrightarrow a \equiv b \pmod{m}$$

La respuesta es claramente negativa porque, por ejemplo,

$$2 \cdot 2 \equiv 0 \cdot 2 \pmod{4} \quad \text{y} \quad 2 \not\equiv 0 \pmod{4}$$

En general, si $1 < d = \text{mcd}(x, m)$, $x = x'd$, $m = m'd$, entonces $m'x \equiv 0 \cdot x \pmod{m}$ y $m' \not\equiv 0 \pmod{m}$ porque $0 < m' < m$.

Lo positivo de esta situación es que se verifica la propiedad cancelativa con multiplicador x si y sólo si $\text{mcd}(x, m) = 1$. Acabamos de ver que, si este máximo común divisor es mayor que 1 nunca se verifica la propiedad cancelativa. Veamos que sí se verifica cuando es 1. Sea $ax \equiv bx \pmod{m}$ y $\text{mcd}(x, m) = 1$. Por la identidad de Bézout existen $\alpha, \beta \in \mathbf{Z}$ tales que $\alpha x + \beta m = 1$. Así, $a = \alpha a x + \beta a m$, $b = \alpha b x + \beta b m$, luego

$$a - b = \alpha(ax - bx) + \beta(a - b)m,$$

que es múltiplo de m. Por tanto, $a \equiv b \pmod{m}$.

Proposición.– La ecuación en congruencias

$$ax \equiv b \pmod{m}$$

tiene solución si y sólo si $d = \text{mcd}(a, m)$ divide a b.

Demostración.– Supongamos que $d|b$, $b = dc$. La identidad de Bézout nos dice que $d = \alpha a + \beta m$, luego $b = dc = \alpha ac + \beta mc$. Como $mc \equiv 0 \pmod{m}$, se tiene que $\alpha ac \equiv b \pmod{m}$, es decir, αc es solución de la ecuación.

Para la implicación contraria supongamos que x_0 es una solución de la ecuación en congruencias. Es decir $ax_0 - b = km$, luego $d|ax_0 - km = b$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

2.4. Clases de congruencias módulo m.

Fijemos un entero $m \geq 2$, y sea $\mathbf{Z}m$ el conjunto de los enteros múltiplos de m.

Sabemos que la relación "ser congruente módulo m" es una relación de equivalencia en el conjunto de los números enteros $\mathbf{Z}$. Por tanto, dicha relación induce una partición en $\mathbf{Z}$ en clases de equivalencia, que llamaremos clases de congruencia módulo m.

Veamos cómo es la clase de equivalencia de un entero $a \in \mathbf{Z}$. Sabemos que $b \in \mathbf{Z}$ está en la clase de a si y sólo si b es congruente con a módulo m, es decir, $m|(b - a)$, luego $b = a + qm$. Por tanto, la clase de congruencia módulo m de a es el conjunto de los enteros de la forma $a + km$, con $k \in \mathbf{Z}$.

Así, dado $a \in \mathbf{Z}$, la clase de congruencia módulo m la denotaremos por $a + \mathbf{Z}m$, y al conjunto de todas las clases de congruencia módulo m lo denotaremos por $\mathbf{Z}/\mathbf{Z}m$.

Vamos a describir el conjunto $\mathbf{Z}/\mathbf{Z}m$ y a ver que podemos sumar y multiplicar los elementos de $\mathbf{Z}/\mathbf{Z}m$.

Proposición.– Todo número natural es congruente módulo m a uno (y sólo uno) de los enteros del conjunto $\{0, 1, 2, \ldots, m - 1\}$.

Demostración.– Sea $a \in \mathbf{N}$. El teorema de la división implica que $a = qm + r$, $0 \leq r < m$. La primera igualdad nos dice que a y r son congruentes módulo m. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Corolario.– Todo número entero es congruente módulo m a uno (y sólo uno) de los enteros del conjunto $\{0, 1, 2, \ldots, m - 1\}$.

Observación.– Así, el conjunto de las clases de congruencias módulo m es

$$\mathbf{Z}/\mathbf{Z}m = \{0 + \mathbf{Z}m, 1 + \mathbf{Z}m, \ldots, (m-1) + \mathbf{Z}m\}.$$

Veamos cómo se definen la suma y el producto de clases de congruencias.

Definición.– Sean $a + \mathbf{Z}m, b + \mathbf{Z}m \in \mathbf{Z}/\mathbf{Z}m$ dos clases de congruencias.

$$(a + \mathbf{Z}m) + (b + \mathbf{Z}m) := (a + b) + \mathbf{Z}m$$

$$(a + \mathbf{Z}m) \cdot (b + \mathbf{Z}m) := (ab) + \mathbf{Z}m.$$

Proposición.– El conjunto $\mathbf{Z}/\mathbf{Z}m$, con las operaciones definidas anteriormente, es un anillo (abeliano).

Ejemplo.– Supongamos que $m = 10, a = 7, b = 9$. Entonces

$$(7 + \mathbf{Z}10) + (9 + \mathbf{Z}10) = 16 + \mathbf{Z}10, (7 + \mathbf{Z}10) \cdot (9 + \mathbf{Z}10) = 63 + \mathbf{Z}10.$$

Teniendo en cuenta que $7 + \mathbf{Z}10 = 17 + \mathbf{Z}10$, $9 + \mathbf{Z}10 = 29 + \mathbf{Z}10$, ¿que ocurre si cambiamos el 7 por 17 y el 9 por 29? No pasa nada, ya que el resultado es el mismo: $(17 + \mathbf{Z}10) + (29 + \mathbf{Z}10) = 46 + \mathbf{Z}10$, pero $46 + \mathbf{Z}10 = 16 + \mathbf{Z}10$. Lo mismo ocurre con el producto.

En la sección anterior probamos que las congruencias módulo m eran compatibles con la suma y el producto, es decir, la suma y el producto que hemos definido no dependen del representante que uno elija.

Hemos visto que toda clase de congruencia $a + \mathbf{Z}m$ es igual a una clase $r + \mathbf{Z}m$, con $0 \leq r < m$. A partir de este momento siempre que trabajemos con clases de congruencias módulo m la escribiremos usando un representante $r, 0 \leq r < m$. Así, pondremos $(7 + \mathbf{Z}10) \cdot (9 + \mathbf{Z}10) = 3 + \mathbf{Z}10$, ya que, por el teorema de división, $63 = 6.10 + 3$, luego 3 es congruente con 63 módulo 10, es decir, $3 + \mathbf{Z}10 = 63 + \mathbf{Z}10$. Análogamente $-11 + \mathbf{Z}10 = 9 + \mathbf{Z}10$.

Ejemplo.– Como ejemplo escribimos las tablas de sumar y de multiplicar de las congruencias módulos 4 y 5.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

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

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Teorema chino del resto.– Sean $m_1, m_2, \ldots, m_n$ enteros, mayores que 1, primos entre sí dos a dos, $a_1, a_2, \ldots, a_n \in \mathbf{Z}$. El sistema de congruencias:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

tiene solución. Además, si x y x' son dos soluciones, entonces $x \equiv x' \pmod{M}$, donde $M = m_1 m_2 \cdots m_n$. Recíprocamente, si x es una solución y $x' \equiv x \pmod{M}$, entonces x' es solución.

Demostración.– Denotemos $M_i = M/m_i$, $\forall i = 1, \ldots, n$. Es claro que

$$\text{mcd}(m_i, M_i) = 1, \quad \forall i = 1, \ldots, n,$$

luego, por la identidad de Bézout, existen $\alpha_i, \beta_i \in \mathbf{Z}$ verificando

$$1 = \alpha_i m_i + \beta_i M_i, \quad i = 1, \ldots, n.$$

Tomemos $x = a_1\beta_1 M_1 + a_2\beta_2 M_2 + \cdots + a_n\beta_n M_n$ y comprobemos que x es solución. Para ello tendremos que comprobar que $x \equiv a_i \pmod{m_i}$, para todo i, o, equivalentemente, que $x - a_i \equiv 0 \pmod{m_i}$, para todo i. Usando la identidad de Bézout correspondiente, tenemos $a_i = a_i\alpha_i m_i + a_i\beta_i M_i$. Entonces,

$$\begin{aligned} x - a_i &= a_1\beta_1 M_1 + \cdots + a_n\beta_n M_n - a_i\alpha_i m_i - a_i\beta_i M_i = \\ &= a_1\beta_1 M_1 + \cdots + a_{i-1}\beta_{i-1} M_{i-1} + a_{i+1}\beta_{i+1} M_{i+1} + \cdots + a_n\beta_n M_n - a_i\alpha_i m_i, \end{aligned}$$

y, al ser todos los sumandos múltiplos de m_i, es $x - a_i \equiv 0 \pmod{m_i}$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

2.5. Los teoremas de Fermat y Euler.

Terminamos este tema probando dos teoremas muy importantes, debidos a Fermat y Euler, así como varios criterios de divisibilidad sencillos, y probablemente conocidos.

Sean m, n enteros positivos. Recordamos que el número combinatorio $\binom{m}{n}$ está definido de la forma siguiente:

$$\binom{m}{n} = \frac{m!}{n!(m-n)!}$$

Lema.– Si p es primo, entonces p divide a $\binom{p}{r}$, para todo $0 < r < p$.

Demostración.– Sabemos que

$$\binom{p}{r} = \frac{p!}{r!(p-r)!}$$

es un entero. Como $1 \leq r \leq p-1$, p no divide a $r!$ ni a $(p-r)!$, los enteros p y $r!(p-r)!$ son primos entre sí. Por tanto $r!(p-r)!$ divide a $(p-1)!$ y

$$\binom{p}{r} = p\left[\frac{(p-1)!}{r!(p-r)!}\right]$$

es un entero múltiplo de p. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Corolario.– Si p es primo, entonces, $\forall a, b \in \mathbf{Z}$, $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Teorema.– Si p es primo, entonces, $\forall a \in \mathbf{Z}$, $a^p \equiv a \pmod{p}$.

Demostración.– Basta probarlo para enteros positivos. Lo haremos por inducción. Para $a = 1$ ya está. Supongamos el teorema cierto para a. Entonces

$$(a+1)^p \equiv a^p + 1^p \equiv a + 1 (\text{mod } p)$$

por la hipótesis de inducción. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

(Pequeño) Teorema de Fermat.– Si p es primo y no divide a $a \in \mathbf{Z}$, entonces $a^{p-1} \equiv 1 \pmod{p}$.

Demostración.– Por el teorema anterior, $a^p \equiv a \pmod{p}$. Por ser p y a primos entre sí, se verifica la propiedad cancelativa, luego $a^{p-1} \equiv 1 \pmod{p}$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– El teorema de Euler está relacionado con las congruencias invertibles módulo m, esto es, los elementos $a + \mathbf{Z}m$ tales que existe $b + \mathbf{Z}m$ verificando

$$(a + \mathbf{Z}m) \cdot (b + \mathbf{Z}m) = 1 + \mathbf{Z}m.$$

Los elementos que verifican esta propiedad se denominan *unidades* módulo m.

Proposición.– $a + \mathbf{Z}m$ es una unidad en $\mathbf{Z}/\mathbf{Z}m$ si y sólo si $\text{mcd}(a, m) = 1$.

Demostración.– Supongamos que $a + \mathbf{Z}m$ es unidad. Entonces existe $b + \mathbf{Z}m$ tal que $(a + \mathbf{Z}m)(b + \mathbf{Z}m) = 1 + \mathbf{Z}m$, luego $ab - 1 = qm$, y $ab - qm = 1$, por tanto a y m son primos entre sí.

Recíprocamente, supongamos que $\text{mcd}(a, m) = 1$. Por la identidad de Bezout existen enteros r, s con $ra + sm = 1$. Luego $1 + \mathbf{Z}m = (ra + sm) + \mathbf{Z}m = (ra + \mathbf{Z}m) + (sm + \mathbf{Z}m) = (a + \mathbf{Z}m)(r + \mathbf{Z}m)$. Por tanto $a + \mathbf{Z}m$ es una unidad. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Corolario.– El conjunto $\mathbf{Z}/\mathbf{Z}p$ es un cuerpo si y sólo si p es primo

Observación.– La notación estándar para el cuerpo $\mathbf{Z}/\mathbf{Z}p$ es $\mathbf{F}_p$, aunque en estos apuntes seguiremos con la notación de congruencias.

Corolario.– El número de unidades de $\mathbf{Z}/\mathbf{Z}m$ es igual al número de enteros $a, 1 \leq a < m$, que son primos con m.

Definición.– Al número de enteros $a, 1 \leq a < m$, que son primos con m se le denota por $\phi(m)$, la *función ϕ de Euler*.

Teorema de Euler.- Sea $a + \mathbf{Z}m$ una unidad en $\mathbf{Z}/\mathbf{Z}m$. Entonces

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Demostración.– Sea

$$P = \{u_1, u_2, \ldots, u_{\phi(m)}\}$$

las unidades de $\mathbf{Z}/\mathbf{Z}m$. Sea

$$Q = \{u_1 a, u_2 a, \ldots, u_{\phi(m)} a\}$$

el conjunto obtenido al multiplicar los elementos de p por a. Es claro que los elementos de Q son todos distintos y son unidades en $\mathbf{Z}/\mathbf{Z}m$. Por tanto los elementos de P y Q son congruentes entre sí (en diferente orden), de donde

$$\prod_{i=1}^{\phi(m)} u_i \equiv \prod_{i=1}^{\phi(m)} u_i a \pmod{m}$$

Si ponemos $u = \prod_{i=1}^{\phi(m)} u_i$ se tiene $u \equiv u a^{\phi(m)} \pmod{m}$. Como u y m son primos entre sí, se verifica la propiedad cancelativa y obtenemos

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Vamos a ver por último, cómo hallar $\phi(m)$ sin necesidad de comprobar elemento a elemento de $\{0, ..., m-1\}$ si son primos con m o no. Para ello no necesitamos más que la factorización de m (en realidad, sólo el conjunto de primos que dividen a m, que es algo menos preciso).

Proposición.– La función ϕ verifica las siguientes propiedades:

1. Si p es primo, entonces $\phi(p) = p - 1$.
2. Si p es primo, entonces $\phi(p^n) = p^n - p^{n-1} = p^n(1 - 1/p)$.
3. Si m y n son primos entre sí, entonces $\phi(nm) = \phi(n)\phi(m)$.
4. Si $n = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$ es la descomposición en factores primos de n, entonces

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right).$$

Demostración.– Los apartados primero y segundo son elementales. El primero es directo y el segundo se sigue de observar que, los únicos números menores que p^n y no primos con él son precisamente los múltiplos de p menores y hay, precisamente p^{n-1} de éstos.

Para ver el tercer apartado, denotemos U_r las unidades mod r y definimos

$$\begin{array}{rcl} f : U_{mn} & \longrightarrow & U_m \times U_n \\ x & \longmapsto & (x, x) \end{array} \qquad \begin{array}{rcll} g : U_m \times U_n & \longrightarrow & U_{mn} & \\ (a, b) & \longmapsto & x \text{ tal que} & x \equiv a \pmod{m} \\ & & & x \equiv b \pmod{n} \end{array}$$

Notemos que, dado que $\text{mcd}(m, n) = 1$, un entero es primo con mn si y sólo si lo es con m y n a la vez. Por tanto f está bien definida, y también lo está g (utilizando el Teorema chino del resto). Es sencillo ver que f y g son aplicaciones inversas la una de la otra, por lo que

$$\phi(mn) = \sharp\,(U_{mn}) = \sharp\,(U_m \times U_n) = \phi(m)\phi(n).$$

El cuarto apartado se sigue directamente del segundo y del tercero. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Tema 3. Polinomios.

3.1. Introducción.

Sea k ($\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}/\mathbf{Z}p$) un cuerpo. Denotaremos por $k[x]$ al conjunto de todas las expresiones de la forma

$$a(x) = \sum_{i=0}^{m} a_i x^i$$

con $a_i \in k$. Así, $k[x]$ denota el conjunto de todos los polinomios con coeficientes en k.

Definición.– El *grado*, notado grado$(a(x))$, de un polinomio no nulo $a(x)$ es el mayor entero n tal que $a_n \neq 0$. El polinomio con $a_0 = a_1 = \ldots = a_m = 0$ se denomina *polinomio nulo* y se denota por 0. Se conviene que grado$(0) = -\infty$.

Sea $a(x) = \sum_{i=0}^{n} a_i x^i \in k[x]$ un polinomio no nulo con $a_n \neq 0$. Llamaremos *término líder* de $a(x)$ al término $a_n x^n$, *coeficiente líder* a a_n y *término constante* a a_0. Un polinomio se dice *mónico* si su coeficiente líder es 1. Los polinomios de grado cero, así como el polinomio nulo, se dicen *polinomios constantes*.

Los polinomios se pueden sumar y multiplicar, extendiendo las operaciones de k. Si $a(x) = \sum_{i=0}^{n} a_i x^i$, $b(x) = \sum_{i=0}^{m} b_i x^i$, suponiendo $m > n$, es

$$a(x) + b(x) = \sum_{i=0}^{n} (a_i + b_i) x^i + b_{n+1} x^{n+1} + \ldots + b_m x^m.$$

El producto de los polinomios $a(x)$ y $b(x)$ está definido por:

$$d(x) = a(x)b(x) = \sum_{l=0}^{m+n} d_l x^l, \quad \text{donde} \quad d_l = \sum_{i+j=l} a_i b_j.$$

Es fácil comprobar que la suma y el producto de polinomios verifican las propiedades conmutativa, asociativa, distributiva, elemento neutro, elemento simétrico y elemento unidad. Esto es, $k[x]$ es un anillo conmutativo. Pero éste no es el único parecido con $\mathbf{Z}$.

Teorema de división.– Sean $f(x), g(x) \in k[x]$ dos polinomios con $g(x) \neq 0$. Existen $q(x), r(x) \in k[x]$, únicos, tales que

$$f(x) = q(x)g(x) + r(x)$$

y grado$(r(x)) <$ grado$(g(x))$.

Demostración.– La demostración se hace de manera efectiva, indicando cómo se calculan cociente y resto de la división euclídea. Si grado$(f(x)) <$ grado$(g(x))$ se pone $q(x) = 0$, $r(x) = f(x)$, y ya hemos terminado nuestra construcción.

Supongamos que grado$(f(x)) \geq$ grado$(g(x))$ y sean ax^m, bx^n los términos de mayor grado de $f(x), g(x)$, respectivamente. Escribamos

$$f_1(x) = f(x) - (a/b)x^{m-n}g(x);$$

entonces $f_1(x)$ es un polinomio de grado estrictamente inferior al de $f(x)$.

Aplicando el mismo razonamiento a $f_1(x)$, y así sucesivamente, logramos crear un conjunto finito de igualdades del tipo

$$\begin{array}{rcl} f(x) & = & q_1(x)g(x) + f_1(x) \\ f_1(x) & = & q_2(x)g(x) + f_2(x) \\ \vdots & & \vdots \\ f_{t-1}(x) & = & q_t(x)g(x) + f_t(x), \end{array}$$

donde

$$\text{grado}(f_1(x)) > \text{grado}(f_2(x)) > \ldots > \text{grado}(f_t(x))$$

y $f_t(x) = 0$ o es de grado inferior al de $g(x)$. Poniendo

$$q(x) = \sum_{i=1}^{t} q_i(x) \ , \ r(x) = f_t(x)$$

se tiene $f(x) = q(x)g(x) + r(x)$.

La unicidad se prueba así: sean

$$f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x);$$

entonces

$$r(x) - r'(x) = (q'(x) - q(x))g(x),$$

con lo que debe ser $r(x) - r'(x) = 0$ porque todo múltiplo no nulo de $g(x)$ tiene que ser de grado mayor o igual que él. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Teorema del resto.– Si $f(x)$ es un polinomio con coeficientes en un cuerpo k, y $a \in k$, entonces $f(a)$ es el resto de dividir $f(x)$ por $x - a$.

Demostración.– Por el teorema de división es

$$f(x) = (x - a)q(x) + r(x) \text{ con grado}(r(x)) < \text{grado}(x - a) = 1.$$

Así, $r(x)$ es una constante, digamos r. Luego $f(a) = (a - a)q(a) + r = r$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Teorema de la raíz.– Sea $f(x) \in k[x]$ un polinomio de grado positivo. Entonces $f(x)$ tiene una raíz $a \in k$ (i.e. existe a en k tal que $f(a) = 0$) si y sólo si es divisible por $x - a$.

Demostración.– En efecto, se puede escribir $f(x) = q(x)(x - a) + r$ con $r \in k$. Así $f(a) = 0$ si y sólo si $r = 0$, lo que equivale a que $(x - a)|f(x)$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Corolario (D'Alembert).– Un polinomio no nulo $f(x) \in k[x]$ de grado n tiene a lo más n raíces distintas en k.

Demostración.– Lo probaremos por inducción en n, el grado de $f(x)$.

Si grado$(f(x)) = 0$, entonces $f(x)$ en un polinomio constante no nulo, luego no tiene raíces en k.

Supongamos que $f(x)$ es un polinomio de grado $n > 0$ y que tiene r raíces distintas $a_1, \ldots, a_r$ en k. Veamos que $r \leq n$.

Tenemos que $f(a_r) = 0$, luego por el teorema de la raíz $f(x) = (x - a_r)g(x)$, con grad$(g(x)) = n - 1$. Para cada $i, 1 \leq i \leq r - 1$, $f(a_i) = 0 = (a_i - a_r)g(a_i)$. Como $a_i \neq a_r$, es $g(a_i) = 0$. Por tanto $a_1, \ldots, a_{r-1}$ son raíces de $g(x)$ y grado$(g(x)) = n - 1$. Por inducción, $r - 1 \leq n - 1$, y $r \leq n$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

3.2. Máximo común divisor.

Con el teorema de división para polinomios podemos, al igual que se hizo con los enteros, dar un algoritmo de Euclides y la identidad de Bézout.

Definición.– Sean $f(x), g(x) \in k[x]$. Un polinomio $p(x) \in k[x]$ es un *máximo común divisor* de $f(x)$ y $g(x)$ si verifica:

1) $p(x)|f(x)$ y $p(x)|g(x)$

2) si $q(x)$ es otro polinomio que divide a $f(x)$ y a $g(x)$ entonces $q(x)|p(x)$.

Observación.– Si $p(x) = \text{mcd}(f(x), g(x))$, entonces, $\forall a \in k \setminus \{0\}$, se tiene que $ap(x) = \text{mcd}(f(x), g(x))$. Por eso cuando hablamos de un máximo común divisor, sobreentenderemos que estamos tomando un polinomio mónico y, en esas condiciones, es único.

Podemos calcular un máximo común divisor de dos polinomios usando el teorema de división, como en los enteros.

Sean $f(x), g(x) \in k[x]$; sabemos que existen $q(x), r(x) \in k[x]$ tales que

$$f(x) = q(x)g(x) + r(x), \quad \text{con grado}(r(x)) < \text{grado}(g(x)).$$

Proposición.– Con las notaciones anteriores, se tiene que

$$\text{mcd}(f(x), g(x)) = \text{mcd}(g(x), r(x))$$

Demostración.– Supongamos que

$$a(x) = \text{mcd}(g(x), r(x)), b(x) = \text{mcd}(f(x), g(x)).$$

Como $f(x) = q(x)g(x) + r(x)$, se tiene que $a(x)|f(x)$ y así $a(x)$ es un divisor común de $f(x)$ y $g(x)$, luego $a(x)|b(x)$.

Análogamente, como

$$r(x) = f(x) - q(x)g(x),$$

se tiene que $b(x)|r(x)$ y así es un divisor común de $g(x)$ y $r(x)$, luego $b(x)|a(x)$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Teorema (Algoritmo de Euclides).– Dados $f(x), g(x) \neq 0 \in k[x]$, grado$(f(x)) >$ grado$(g(x))$, hacemos divisiones sucesivas, y obtenemos:

$$\begin{array}{rcl} f(x) & = & q(x)g(x) + r(x) \\ g(x) & = & q_0(x)r(x) + r_1(x) \\ r(x) & = & q_1(x)r_1(x) + r_2(x) \\ & \vdots & \\ r_{n-2}(x) & = & q_{n-1}(x)r_{n-1}(x) + r_n(x) \\ r_{n-1}(x) & = & q_n(x)r_n(x) \end{array}$$

Entonces el proceso es finito y, con las notaciones anteriores, mcd$(f(x), g(x)) = r_n(x)$.

Demostración.– Consideremos la sucesión $\{\text{grado}(r_i(x))\}$ que es una sucesión estrictamente decreciente de enteros no negativos. Como el primer elemento es grado$(f(x))$, la sucesión puede tener a lo más grado$(f(x)) + 1$ elementos. Por tanto, existe un $n \geq 1$ tal que $r_{n+1}(x) = 0$.

Por el lema anterior tenemos que:

$$\text{mcd}(f(x), g(x)) = \text{mcd}(g(x), r_2(x)) = \ldots = \text{mcd}(r_{n-1}(x), r_n(x)) = r_n(x).$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Teorema (Identidad de Bézout).– Sean $a(x), b(x) \in k[x]$, $b(x) \neq 0$. Si denotamos mcd$(a(x), b(x)) = d(x)$ entonces existen elementos $s(x), t(x) \in k[x]$ tales que

$$d(x) = s(x)a(x) + t(x)b(x).$$

Demostración.– La demostración es consecuencia del algoritmo de Euclides.

3.3. Factorización. Factores múltiples.

Definición.– Diremos que un polinomio $p(x) \in k[x]$ es *irreducible* si no es una constante, y si $p(x) = f(x)g(x)$, entonces $f(x)$ o $g(x)$ es una constante.

Los polinomios irreducibles juegan en $k[x]$ el mismo papel que los números primos en **Z**.

Proposición.– Sea $p(x) \in k[x]$ irreducible. Si $f(x)$ es un polinomio que no es divisible por $p(x)$, entonces el máximo común divisor de $p(x)$ y $f(x)$ es 1.

Demostración.– Sea $d(x) = \text{mcd}(p(x), f(x))$. Sabemos que $p(x)$ no divide a $f(x)$, entonces

$$f(x) = q(x)p(x) + r(x), \text{ con } 0 < \text{grado}(r(x)) < \text{grado}(p(x)) \text{ y } r(x) \neq 0,$$

y además grado$(d(x)) <$ grado$(p(x))$, pues $d(x)|r(x)$. Como $d(x)|p(x)$ y $p(x)$ es irreducible, o bien $d(x)$ es una constante no nula o es $d(x) = p(x)$. Esto último es imposible por los grados así, $d(x)$ es una constante no nula. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Teorema.– Cualquier polinomio de grado ≥ 1 de $k[x]$ es irreducible o factoriza en producto de polinomios irreducibles.

Teorema.– Sea $p(x) \in k[x]$ irreducible. Si $p(x)|f(x)g(x)$, entonces $p(x)$ divide a $f(x)$ o a $g(x)$.

Teorema.– Sea $f(x) = p_1(x) \dots p_s(x) = q_1(x) \dots q_t(x)$ dos factorizaciones de $f(x)$ en producto de polinomios irreducibles en $k[x]$. Entonces $s = t$ y existe una correspondencia uno a uno entre los factores $p_1(x), \dots, p_s(x)$ y $q_1(x), \dots, q_t(x)$ donde, si $p_i(x)$ se corresponde con $q_j(x)$, se tiene que $p_i(x) = \alpha q_j(x)$, para algún $\alpha \in k \setminus \{0\}$.

La demostración de estos tres teoremas es igual que en $\mathbf{Z}$. Sin embargo, una herramienta específica y útil de los polinomios es la derivada, que coincide con el concepto usual de análisis.

Observación.– Usaremos la notación habitual: $f'(x)$ es el polinomio que se obtiene al derivar $f(x)$; $D : k[x] \to k[x]$ es la función que a cada polinomio le asocia su derivada, $D(f(x)) = f'(x)$.

Definición.– La *derivada* de un polinomio $f(x)$ está definida por las siguientes reglas:

1) Si $f(x) = ax^n$, $a \in k$, entonces $D(ax^n) = nax^{n-1}$.

2) Si $f(x) = g(x) + h(x)$, entonces $D(f(x)) = D(g(x)) + D(h(x))$.

Proposición.– Se verifica que:

1) $D(f(x)g(x)) = f(x)D(g(x)) + g(x)D(f(x))$.

2) $D(f(x)^s = sf(x)^{s-1}D(f(x))$.

Teorema.– Sea $f(x) \in k[x]$.

1) Si $f(x)$ tiene factores múltiples, entonces $f(x)$ y $f'(x)$ no son primos entre sí.

2) (característica cero $k = \mathbf{Q}, \mathbf{R}, \mathbf{C}$) Si $f(x)$ y $f'(x)$ no son primos entre sí, entonces $f(x)$ tiene factores múltiples.

Demostración: Supongamos que $f(x)$ tiene algún factor múltiple, $f(x) = p(x)^s q(x)$, con $s > 1$. Entonces

$$f'(x) = p(x)^{s-1}[sp'(x)q(x) + p(x)q'(x)],$$

luego $p(x)$ es un factor común de $f(x)$ y $f'(x)$.

Sean $d(x) = \text{mcd}(f(x), f'(x))$, que sabemos es de grado mayor que cero, y $p(x)$ un factor irreducible de $d(x)$. Veamos que $p(x)$ es un factor múltiple de $f(x)$.

Como $p(x)|f(x)$, es $f(x) = p(x)g(x)$. Derivando tenemos

$$f'(x) = p'(x)g(x) + p(x)g'(x).$$

Como $p(x)|f'(x)$, $p(x)$ divide al producto $p'(x)g(x)$, y, por ser $p(x)$ irreducible, divide a uno de los factores. Ahora bien, $p(x)$ no puede dividir a $p'(x)$ pues tiene grado estrictamente mayor (característica cero), luego $p(x)|g(x)$, y $g(x) = p(x)h(x)$. Sustituyendo tenemos $f(x) = p(x)^2 h(x)$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

3.4. Congruencias. Teorema chino del resto

Las congruencias para polinomios se definen igual a la de los enteros y tienen propiedades similares.

Definición.– Sea $p(x) \in k[x]$. Dados $f(x), g(x) \in k[x]$, diremos que $f(x)$ y $g(x)$ son *congruentes* módulo $p(x)$, y escribiremos

$$f(x) \equiv g(x) \pmod{p(x)},$$

si $p(x)$ divide a $f(x) - g(x)$.

Observación.– La relación de congruencia mod $p(x)$ tiene las mismas propiedades que la de congruencia módulo m de enteros. Por ejemplo:

- Las congruencias son compatibles con la suma.
- Las congruencias son compatibles con la multiplicación.
- La congruencia es una relación de equivalencia en $k[x]$.

De la misma forma que construimos los anillos $\mathbf{Z}/\mathbf{Z}m$ de las clases de congruencias módulo m, podemos considerar el conjunto de las clases de congruencias de polinomios de $k[x]$ módulo $m(x)$, que lo denotaremos por $k[x]/(m(x))$.

Proposición.– Si $m(x)$ tiene grado d, cualquier clase de congruencia módulo $m(x)$ tiene un único representante $r(x)$ de grado estrictamente menor que d.

Demostración.– Sea $f(x) \in k[x]$. Por el algoritmo de división tenemos que

$$f(x) = q(x).m(x) + r(x), \quad \text{grado}(r(x)) < \text{grado}(m(x))$$

y $f(x) \equiv r(x) \pmod{m(x)}$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Esto prueba que el conjunto de polinomios de $k[x]$ de grado estrictamente menor que el grado de $m(x)$ es un conjunto completo de representantes para $k[x]/(m(x))$.

Ejemplo.– Sea $m(x) = x^2 + 1 \in \mathbf{Q}[x]$. Cada elemento de $\mathbf{Q}[x]/(m(x))$ tiene un representante de grado menor o igual que 1. Como

$$x^2 \equiv -1 \pmod{x^2 + 1},$$

es

$$x^3 \equiv -x \pmod{x^2 + 1}.$$

En general, es fácil ver que

$$x^{2n} \equiv (-1)^n \pmod{x^2 + 1}$$

y

$$x^{2n+1} \equiv (-1)^n x \pmod{x^2 + 1}.$$

Como $\mathbf{Q}$ es un cuerpo infinito, existen infinitos polinomios de grado menor o igual que 1 en $\mathbf{Q}[x]$, y por tanto $\mathbf{Q}[x]/(x^2 + 1)$ es un conjunto infinito.

Si cambiamos $\mathbf{Q}$ por $\mathbf{Z}/\mathbf{Z}3$ tenemos que

$$(\mathbf{Z}/\mathbf{Z}3)[x]/(x^2+1) = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}.$$

Observación.– Al igual que hicimos con los enteros, podemos definir la suma y la multiplicación de clases de congruencias de polinomios como la clase definida por la suma y la multiplicación, respectivamente, de sus representantes. Es fácil comprobar que estas operaciones están bien definidas y verifican las propiedades usuales de la suma y la multiplicación, convirtiendo a $k[x]/(m(x))$ en un anillo.

Teorema chino del resto.– Sean $m_1(x), \ldots, m_n(x) \in k[x]$ polinomios primos entre sí dos a dos, $a_1(x), \ldots, a_n(x) \in k[x]$ arbitrarios. Entonces existe $f(x) \in k[x]$ tal que:

$$\begin{array}{rl} f(x) \equiv a_1(x) & (\text{mod } m_1(x)) \\ f(x) \equiv a_2(x) & (\text{mod } m_2(x)) \\ \vdots & \vdots \\ f(x) \equiv a_n(x) & (\text{mod } m_n(x)) \end{array}$$

Si $f_1(x)$ y $f_2(x)$ son dos soluciones, se verifica que:

$$f_1(x) \equiv f_2(x) \pmod{m_1(x)m_2(x)\cdots m_n(x)}.$$

Demostración: La demostración es análoga al caso de los enteros.

Como $m_i(x)$ y $m_j(x)$ son primos entre sí, para todo $i \neq j$, $m_i(x)$ es primo con

$$l_i(x) = m_1(x)\cdots m_{i-1}(x)m_{i+1}(x)\cdots m_n(x).$$

Por la identidad de Bézout, existen $\alpha_i(x), \beta_i(x) \in k[x]$ tales que

$$1 = \alpha_i(x)m_i(x) + \beta_i(x)l_i(x), \quad \forall i = 1, \ldots, n.$$

Se tiene que

$$\begin{array}{l} \beta_i(x)l_i(x) \equiv 1 \pmod{m_i(x)} \\ \beta_i(x)l_i(x) \equiv 0 \pmod{m_j(x)}, \quad \forall i \neq j \end{array}$$

La solución es entonces

$$f(x) = a_1(x)\beta_1(x)l_1(x) + a_2(x)\beta_2(x)l_2(x) + \ldots + a_n(x)\beta_n(x)l_n(x).$$

3.5. Factorización en $\mathbf{C}[x]$ y en $\mathbf{R}[x]$

El resultado que enunciamos a continuación, y cuya demostración puede verse en *Lindsay Childs, A Concrete Introduction to Higher Algebra* nos dice cómo son los polinomios irreducibles sobre $\mathbf{C}$.

Teorema fundamental del álgebra.– Todo polinomio $f(x) \in \mathbf{C}[x]$ de grado positivo tiene una raíz en $\mathbf{C}$.

Corolario.– Todo polinomio $f(x) \in \mathbf{C}[x]$ de grado positivo, digamos n, tiene n raíces en $\mathbf{C}$, i.e, se puede escribir

$$f(x) = \alpha \prod_{i=1}^{n} (x - \alpha_i),$$

donde $\alpha, \alpha_i \in \mathbf{C}$.

Demostración.– Por el teorema fundamental del álgebra, $f(x)$ tiene una raíz α_1 en $\mathbf{C}$. Se puede, pues, escribir, $f(x) = (x - \alpha_1) f_1(x)$. Aplicando el mismo razonamiento a $f_1(x)$, y así sucesivamente, se llega, después de $n - 1$ pasos a una expresión de la forma

$$f(x) = (x - \alpha_1) \dots (x - \alpha_{n-1}) f_{n-1}(x),$$

donde $f_{n-1}(x)$ es un polinomio de primer grado. Como $f_{n-1}(x)$ se puede escribir $f_{n-1}(x) = \alpha x - \alpha\alpha_n$, se tiene el resultado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Por tanto, los únicos polinomios irreducibles en $\mathbf{C}[x]$ son los de grado 1. Veamos cómo son los polinomios irreducibles en $\mathbf{R}[x]$.

Proposición.– Todo polinomio de $\mathbf{R}[x]$ de grado impar tiene una raíz en $\mathbf{R}$. Todo polinomio de grado par se descompone en producto de polinomios de grados 1 ó 2 (los cuales son irreducibles si y sólo si sus raíces son complejas no reales).

Demostración.– Sea $f(x) \in \mathbf{R}[x]$ un polinomio de grado positivo, digamos n. Por el teorema fundamental del álgebra, $f(x)$ tiene n raíces en $\mathbf{C}$. Sea

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \ , \ a_i \in \mathbf{R} \ \forall i = 0, 1, \dots, n,$$

y sea $\alpha = a + bi$ una raíz. De

$$0 = f(\alpha) = a_0 (a + bi)^n + a_1 (a + bi)^{n-1} + \dots + a_{n-1}(a + bi) + a_n$$

se deduce, tomando conjugados, que

$$0 = \overline{f(\alpha)} = f(\overline{\alpha}) = a_0 (a - bi)^n + a_1 (a - bi)^{n-1} + \dots + a_{n-1}(a - bi) + a_n.$$

Así pues, si α es una raíz de $f(x)$, también lo es $\overline{\alpha}$. Por tanto, las raíces no reales de $f(x)$ aparecen por pares de conjugadas. Si n es impar, tiene que haber una raíz que coincida con su conjugada, luego es real. Esto prueba el primer aserto.

En cuanto al segundo aserto, se prueba así. Si $\alpha = a + bi$ es una raíz compleja no real de $f(x)$, el polinomio

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - 2ax + (a^2 + b^2)$$

divide a $f(x)$ y tiene coeficientes reales. De aquí es obvia la conclusión. Esto prueba el resultado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

3.6. Factorización en $\mathbf{Q}[x]$.

Observación.– Sea $f(x) \in k[x]$ un polinomio de grado 2 ó 3. Entonces $f(x)$ es reducible si y sólo si tiene una raíz en k. En efecto, el hecho de que $f(x)$ sea reducible es equivalente

a decir que tiene un divisor que es de grado 1. Si éste es $ax - b$, entonces b/a es una raíz de $f(x)$.

Naturalmente, lo anterior no funciona para grados mayores. Un polinomio de grado 4 se puede descomponer, por ejemplo, en dos factores irreducibles de grado 2, luego no tiene por qué tener raíces en k. Con mayor razón ocurrirá esto en grados más altos. No obstante es bueno ver si un polinomio dado tiene o no raíces en k. Si las tiene, y es de grado mayor que 1, es automáticamente reducible.

Observación.– Consideremos el caso de $k = \mathbf{Q}$. El problema de saber cuándo un polinomio de $\mathbf{Q}[x]$ es irreducible es muy difícil de resolver. Sin embargo, el problema de la localización de raíces (que, como hemos notado, es más simple), sí se puede atacar.

Para empezar, notemos que si $f(x) \in \mathbf{Q}[x]$ es igual buscar sus raíces que las de $af(x)$, donde $a \in \mathbf{Z}$. En particular, podemos suponer que $f(x)$ está, en realidad en $\mathbf{Z}[x]$ (esto es, todos sus coeficientes son enteros). En estas condiciones tenemos el siguiente resultado, también conocido como *Regla de Ruffini*.

Proposición.– Sea

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \ , \ a_i \in \mathbf{Z}, \forall i = 0, 1, \ldots, n$$

un polinomio de grado $n > 0$. Supongamos que $f(x)$ tiene una raíz racional $\alpha = a/b$ con $\text{mcd}(a, b) = 1$. Entonces $a|a_n$ y $b|a_0$.

Demostración.– En efecto, de

$$0 = f(a/b) = a_0(a/b)^n + a_1(a/b)^{n-1} + \ldots + a_{n-1}(a/b) + a_n$$

se deduce, previa multiplicación por b^n, que

$$0 = a_0a^n + a_1a^{n-1}b + \ldots + a_{n-1}ab^{n-1} + a_nb^n.$$

Como a divide a todos los términos, salvo al último, y es primo con b, debe dividir a a_n. Como b divide a todos los términos, salvo al primero, y es primo con a, debe dividir a a_0. Esto prueba el aserto. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Para atacar el problema de la factorización nos reduciremos primero, de nuevo, al caso de los polinomios con coeficientes enteros, donde la factorización única de los coeficientes nos puede ser de ayuda.

Definición.– Dado $f(x) \in \mathbf{Z}[x]$ no nulo, se llama *contenido de* $f(x)$ al máximo común divisor de sus coeficientes. Se representará por $c(f)$. Se dirá que $f(x)$ es *primitivo* si su contenido es 1.

Lema de Gauss.– El producto de dos polinomios primitivos es primitivo.

Demostración.– Sean

$$f(x) = a_mx^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0 \ , \ a_i \in \mathbf{Z}, \forall i = 0, 1, \ldots, m,$$

$$g(x) = b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0 \ , \ b_i \in \mathbf{Z}, \forall i = 0, 1, \ldots, n$$

dos polinomios primitivos. Para probar que $f(x)g(x)$ es primitivo basta ver que, fijado $p \in \mathbf{Z}$, irreducible, existe un coeficiente de $f(x)g(x)$ que no es divisible por él.

Fijemos, pues, p irreducible. Sea s (resp t) el entero $0 \leq s \leq m$ (resp. $0 \leq t \leq n$) tal que $p|a_i$ para todo $i > s$ (resp. $p|b_j$ para todo $j > t$), si hay caso, y p no divide a a_s (resp. a b_t). El coeficiente de x^{s+t} en $f(x)g(x)$ es

$$a_0b_{s+t} + \ldots + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + \ldots + a_{s+t}b_0,$$

en el que se ve que p divide a todos los sumandos salvo a a_sb_t. Así, p no divide a la suma, lo que prueba el resultado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Corolario.– Si $f(x), g(x) \in \mathbf{Q}[x]$ son polinomios no nulos, entonces

$$c(fg) = c(f)c(g).$$

Demostración.– Se puede escribir

$$f(x) = c(f)f'(x), \quad g(x) = c(g)g'(x)$$

donde f', g' son primitivos. Así

$$f(x)g(x) = c(f)c(g)f'(x)g'(x)$$

y, como $f'(x)g'(x)$ es primitivo por el lema de Gauss, es $c(f)c(g) = c(fg)$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

El siguiente resultado es sencillo, pero de una importancia extrema cuando se trata de factorizar polinomios.

Corolario.– Sea $f(x) \in \mathbf{Z}[x]$ un polinomio de grado positivo, digamos n, que se descompone en $\mathbf{Q}[x]$ en producto de dos polinomios de grados estrictamente menores que n. Entonces se descompone en $\mathbf{Z}[x]$ en producto de dos polinomios de esos mismos grados.

Demostración.– Sea $f(x) = f_1(x)g_1(x)$, donde $f_1(x), g_1(x) \in \mathbf{Q}[x]$ con $\mathrm{grado}(f_1) < n$ y $\mathrm{grado}(g_1) < n$. Multiplicando la anterior igualdad por un cierto elemento $a \in \mathbf{Z}$, se pueden quitar los denominadores de $f_1(x), g_1(x)$, es decir, se tendrá

$$af(x) = g(x)h(x)\ ,\ g(x), h(x) \in \mathbf{Z}[x].$$

De ahí se deduce que $ac(f) = c(gh) = c(g)c(h)$. Si se pone, $g = c(g)g'$, $h = c(h)h'$, entonces

$$f(x) = \frac{c(g)c(h)}{a}g'(x)h'(x),$$

y ésta es la descomposición buscada. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Corolario.– Sea $f(x) \in \mathbf{Z}[x]$ un polinomio de grado positivo, digamos n, y primitivo. Entonces $f(x)$ es reducible en $\mathbf{Z}[x]$ si y sólo si lo es en $\mathbf{Q}[x]$. Lo mismo ocurre para irreducible.

Demostración.– El resultado es consecuencia inmediata del hecho de que un polinomio primitivo es reducible en $\mathbf{Z}[x]$ si y sólo si se descompone en producto de dos polinomios de grado inferior. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Terminamos la teoría de esta sección con un criterio muy general de irreducibilidad de polinomios, aunque no es concluyente porque no se puede aplicar a todos: es el *criterio de Eisenstein*, que damos a continuación.

Proposición (Criterio de Eisenstein).– Sea

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \ , \ a_i \in \mathbf{Z}, \forall i = 0, 1, \ldots, n,$$

un polinomio de grado $n > 0$. Supongamos que existe un elemento irreducible $p \in \mathbf{Z}$ que divide a todos los coeficientes, salvo a a_n, y tal que p^2 no divide a a_0. Entonces $f(x)$ es irreducible en $\mathbf{Q}[x]$.

Demostración.– Se hará por reducción al absurdo. Supongamos que $f(x)$ fuese reducible en $\mathbf{Q}[x]$; entonces se descompondría, en $\mathbf{Q}[x]$, en producto de dos polinomios de grado estrictamente inferior. Por el corolario anterior se puede escribir

$$f(x) = (b_s x^s + b_{s-1}x^{s-1} + \ldots + b_1 x + b_0)(b'_t x^t + b'_{t-1}x^{t-1} + \ldots + b'_1 x + b'_0)$$

donde $b_i, b'_j \in \mathbf{Z}, \forall i, j$ y $s, t < n$.

Por la segunda hipótesis, p debe dividir a uno de los dos b_0, b'_0, pero no a ambos. Supongamos que $p|b_0$ y no divide a b'_0. Como p no divide a a_n, no puede dividir a todos los b_i. Sea m el mínimo índice tal que p no divide a b_m. El coeficiente del término en x^m es

$$b_m b'_0 + b_{m-1}b'_1 + \ldots + b_0 b'_m = a_m,$$

que no es divisible por p pues todos los sumandos lo son, salvo el primero. Como $m < n$, se tiene una contradicción, lo que prueba el teorema. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Para terminar esta sección veremos, con ejemplos, un procedimiento para descomponer un polinomio, con coeficientes en $\mathbf{Q}$ en producto de sus factores irreducibles.

Observación.– Notemos los siguientes hechos:

1. Todo polinomio $f(x) \in \mathbf{Q}[x]$ se puede escribir como $df(x) = h(x)$, con $d \in \mathbf{Z}$, $h(x) \in \mathbf{Z}[x]$. Por tanto, para obtener la descomposición, en $\mathbf{Q}$, de $f(x)$ puedo calcular la de $h(x)$. Es decir, podemos considerar sólo polinomios con coeficientes enteros.

2. Sea $f(x) \in \mathbf{Z}[x]$. Sabemos que $f(x) = c(f)h(x)$, donde $h(x) \in \mathbf{Z}[x]$ y es primitivo. Para obtener la descomposición, en $\mathbf{Q}$, de $f(x)$ puedo calcular la de $h(x)$. Es decir, podemos considerar sólo polinomios con coeficientes enteros y primitivos.

Ejemplo.– Consideremos el polinomio $f(x) = x^5 + x^3 - 2x^2 - 2 \in \mathbf{Z}[x]$ y primitivo. Si $f(x)$ es reducible se puede poner como producto de dos polinomios (no constantes) $f(x) = h(x)g(x)$, $h(x), g(x) \in \mathbf{Z}[x]$. Como el polinomio de partida es de grado 5, las posibilidades son:

1) grado$(h(x)) = 1$ y grado$(g(x)) = 4$

2) grado$(h(x)) = 2$ y grado$(g(x)) = 3$

Ahora se trata de probar "manualmente" si es posible alguna de las posibilidades. Una respuesta negativa indicaría que el polinomio de partida es irreducible.

El caso (1) es el teorema de Ruffini. Si $h(x) = ax + b$ es de grado 1, entonces $-b/a$ es una raíz de $f(x)$. Por tanto, se dará la posibilidad (1) si y sólo si $f(x)$ tiene raíces

racionales (notemos que este argumento es válido independiente del grado del polinomio de partida).

En nuestro ejemplo sabemos (por Ruffini) que las posibles raíces de $f(x)$ son: $\pm 1, \pm 2$. Sustituyendo en $f(x)$ comprobamos que ninguna es raíz, luego la posibilidad (1) no se da.

Veamos si es posible la segunda. Si lo fuese posible, existirían enteros a, b, c, d, e, f, r tales que:

$$x^5 + x^3 - 2x^2 - 2 = (ax^2 + bx + c)(dx^3 + ex^2 + fx + r)$$

Operando, tenemos $(ax^2 + bx + c)(dx^3 + ex^2 + fx + r) = adx^5 + (ae + bd)x^4 + (af + be + cd)x^3 + (ar + bf + ce)x^2 + (br + cf)x + cr$, y este polinomio será igual a $f(x)$ si tienen los mismos coeficientes. Por tanto, la segunda posibilidad se da si existen unos enteros a, b, c, d, e, f, r tales que:

$$S : \begin{cases} 1 &= ad \\ 0 &= ae + bd \\ 1 &= af + be + cd \\ -2 &= ar + bf + ce \\ 0 &= br + cf \\ -2 &= cr \end{cases}$$

Es decir, tenemos que tratar de resolver, en $\mathbf{Z}$, el sistema de ecuaciones (no lineales) S. La mejor forma es estudiar casos. La primera ecuación nos dice que $a = d = 1$ o $a = d = -1$. Supongamos que $a = d = 1$. Si con esta elección encontramos una solución, ya tendríamos los polinomios $h(x)$ y $g(x)$. En caso contrario tendríamos que resolver el sistema con $a = b = -1$.

Si $a = d = 1$, el sistema anterior es:

$$S : \begin{cases} 0 &= e + b \\ 1 &= f + be + c \\ -2 &= r + bf + ce \\ 0 &= br + cf \\ -2 &= cr \end{cases}$$

De la última ecuación se tiene los siguientes casos: (1) $c = -1, r = 2$, (2) $c = 1, r = -2$, (3) $c = -2, r = 1$ y (4) $c = 2, r = -1$.

Caso (1). El sistema a resolver es

$$S : \begin{cases} 0 &= e + b \\ 1 &= f + be - 1 \\ -2 &= 2 + bf - e \\ 0 &= 2b - f \end{cases}$$

Sustituyendo $e = -b, f = 2b$ en la segunda ecuación se obtiene $b^2 - 2b + 2 = 0$ que no tiene solución entera. Por tanto este caso no se puede dar

Caso (2). El sistema a resolver es

$$S : \begin{cases} 0 &= e + b \\ 1 &= f + be + 1 \\ -2 &= -2 + bf + e \\ 0 &= -2b + f \end{cases}$$

que tiene como solución $e = f = d = 0$.

Por tanto $f(x)$ es reducible y su descomposición es factores irreducibles es $f(x) = (x^2+1)(x^3-2)$. Los polinomios x^2+1 y x^3-2 son irreducibles pues no tienen raíces racionales.

Observación.– Si el polinomio de partida es mónico, podemos suponer que los factores en que se descompone son también mónicos.

3.7. Factorización en $\mathbf{Z}/\mathbf{Z}p[x]$.

Observación.– El mismo procedimiento "artesanal" que usamos en 3.6. para factorizar en $\mathbf{Q}[x]$ se puede usar para obtener la descomposición en factores irreducibles de polinomios con coeficientes en $\mathbf{Z}/\mathbf{Z}p$, con p primo.

Ejemplo.– Consideremos el polinomio $f(x) = x^4 + x^3 + x + 2 \in \mathbf{Z}/\mathbf{Z}3$. Si $f(x)$ es reducible se puede poner como producto de dos polinomios (no constantes) $f(x) = h(x)g(x),\ h(x), g(x) \in \mathbf{Z}/\mathbf{Z}3[x]$. Como el polinomio de partida es de grado 4, las posibilidades son:

1) grado$(h(x)) = 1$ y grado$(g(x)) = 3$

2) grado$(h(x)) = 2$ y grado$(g(x)) = 2$

El caso (1) se resuelve, como en Q, comprobando si $f(x)$ posee alguna raíz en $\mathbf{Z}/\mathbf{Z}3$. Como $\mathbf{Z}/\mathbf{Z}3 = \{0, 1, 2\}$ es finito, basta comprobar si algún elemento es raíz. En nuestro caso $f(0) = 2, f(1) = 2$ y $f(2) = 1$. Luego la posibilidad (1) no se da.

Para estudiar el caso (2) pongamos $f(x) = (x^2 + ax + b)(x^2 + cx + d)$. Operando e igualando coeficientes obtenemos el sistema

$$S : \begin{cases} 1 &= a + c \\ 0 &= b + d \\ 1 &= ad + bc \\ 2 &= bd \end{cases}$$

La segunda ecuación nos dice que $d = 2b$ y sustituyendo en la última, obtenemos que $b^2 = 1$, de donde $b = 1$ o $b = 2$. Para $b = 1$ el sistema a resolver es

$$S : \begin{cases} 1 &= a + c \\ 1 &= 2a + c \end{cases}$$

cuya solución es $a = 0, c = 1$. Por tanto $f(x) = (x^2+1)(x^2+x+2)$ es la descomposición en factores irreducibles (los polinomios x^2+1 y x^2+x+2 son irreducibles pues no tienen raíces en $\mathbf{Z}/\mathbf{Z}3$.)

Para ilustrar la importancia del problema de factorizar sobre $\mathbf{Z}/\mathbf{Z}p[x]$ veamos cómo podemos relacionar la irreducibilidad en $\mathbf{Q}$ y en $\mathbf{Z}/\mathbf{Z}p$, p primo. Sea

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbf{Z}[x]$$

primitivo, p un primo que no divida a a_n, y pongamos

$$\overline{f}(x) = \overline{a}_0 + \overline{a}_1 + \ldots + \overline{a}_n x^n \in \mathbf{Z}/\mathbf{Z}p[x],$$

donde $\overline{a}_i = a_i + \mathbf{Z}p$, $0 \leq i \leq n$.

Proposición.– Si $\overline{f}(x)$ es irreducible en $\mathbf{Z}/\mathbf{Z}p[x]$, entonces $f(x)$ es irreducible en $\mathbf{Q}[x]$.

Demostración.– Elemental $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Veamos, con un ejemplo, cómo podemos usar el resultado anterior.

Ejemplo.– Sea $f(x) = x^4 - x^3 + x^2 - x + 1 \in \mathbf{Z}[x]$. Tomemos $p = 2$. Entonces $\overline{f}(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbf{Z}/\mathbf{Z}2$. $\overline{f}(0) = 1, \overline{f}(1) = 1$, luego $\overline{f}(x)$ no tiene raíces en $\mathbf{Z}/\mathbf{Z}2$.

Si $f(x) = (x^2 + ax + b)(x^2 + cx + d)$. Operando e igualando coeficientes obtenemos el sistema

$$S : \begin{cases} 1 &= a + c \\ 1 &= b + d \\ 1 &= ad + bc \\ 1 &= bd \end{cases}$$

La última ecuación nos dice que $b = d = 1$, y sustituyendo en la segunda obtenemos que $1 = 0$, luego S no tiene solución. Por tanto, $\overline{f}(x)$ es irreducible en $\mathbf{Z}/\mathbf{Z}2$ y, por la proposición, $f(x)$ es irreducible sobre $\mathbf{Q}$.

Observación.– Si bien, aparentemente, este procedimiento simplifica los cálculos a la hora de estudiar si un polinomio es o no irreducible sobre $\mathbf{Q}$, tiene un grave inconveniente. El recíproco de la proposición anterior es falso. Por ejemplo, el polinomio $x^2 + 2$ es irreducible sobre $\mathbf{Q}$, pero $\overline{f}(x) = x^2 \in \mathbf{Z}/\mathbf{Z}2[x]$ es reducible. A modo de ejemplo, el polinomio $x^4 - x^2 + 1$ es irreducible en $\mathbf{Q}$ y $\overline{f}(x)$ es reducible en $\mathbf{Z}/\mathbf{Z}p$ para cualquier primo p (*Lindsay Childs, A concrete introduction to higher algebra*).

3.8. Factorización efectiva en $\mathbf{Q}[x]$ y $\mathbf{Z}/\mathbf{Z}p[x]$ (opcional).

El objetivo de esta lección es dar dos opciones, computacionalmente efectivas y más sofisticadas que las vistas hasta ahora, para atacar el problema de la factorización sobre los racionales (método de los polinomios interpoladores de Lagrange) y sobre los cuerpos primos (método de Berlekamp).

Observación.– Comencemos con el caso de un polinomio $f(x) \in \mathbf{Z}[x]$ de grado n y sea $d = [n/2]$. Obviamente, salvo que $f(x)$ sea irreducible, alguno de sus factores irreducibles ha de tener grado menor o igual que d, por lo que me basta buscar los posibles factores que verifican esta condición.

Para ello fijamos $d + 1$ enteros distintos (normalmente lo más cerca posible de 0, por motivos de comodidad) $a_0, a_1, ..., a_d$ y hallamos

$$n_i = f(a_i), \quad i = 0, ..., d.$$

Obviamente, si $g(x)$ es un factor, del tipo que busco, de $f(x)$, ha de verificar que $s_i = g(a_i)$ divide al n_i correspondiente. Así pues, fijamos una $(d+1)$–upla (vector de

divisores)

$$(s_0, s_1, ..., s_d)\,, \text{ donde } s_i | n_i, \quad i = 0, ..., d.$$

Recordemos que $g(a_i)$ es precisamente $g(x)$ mod $(x - a_i)$. Así pues, por el Teorema chino del resto, $g(x)$ ha de ser entonces una solución al sistema

$$\begin{array}{ll} g(x) \equiv a_0 & \text{mod } (x - a_0) \\ g(x) \equiv a_1 & \text{mod } (x - a_1) \\ \vdots & \vdots \\ g(x) \equiv a_d & \text{mod } (x - a_d) \end{array}$$

y notemos que este sistema tiene solución única de grado menor o igual que d. Así pues, fijado un vector de divisores, tenemos un posible divisor de f. Como los posibles vectores de divisores son finitos, este procedimiento nos da una lista exhaustiva de todos los posibles divisores de $f(x)$ de grado menor o igual que d

Observación.– El algoritmo de Berlekamp para factorizar en $\mathbf{Z}/\mathbf{Z}p[x]$ se basa en el siguiente resultado.

Teorema.– Sea $f(x) \in \mathbf{Z}/\mathbf{Z}p[x]$ de grado n, sin factores múltiples y mónico, y supongamos que existe $g(x)$ tal que

$$f(x) \mid (g(x)^p - g(x))\,.$$

Entonces

$$f(x) = \prod_{s=1}^{p} \text{mcd}\,(f(x), g(x) - s)\,,$$

aunque varios de estos factores pueden ser polinomios constantes.

Demostración.– Notemos, en primer lugar, que en característica p se tiene que

$$x^p - x = \prod_{s=1}^{p} (x - s),$$

lo cual, en particular implica que

$$g(x)^p - g(x) = \prod_{s=1}^{p} (g(x) - s)\,.$$

Todos estos factores son primos entre sí, porque si un polinomio divide a $g(x) - s$ y a $g(x) - t$, con $s \neq t$, debe dividir a $t - s$ y por tanto es constante.

Probemos entonces la igualdad que hemos enunciado. Por un lado, es sencillo ver que

$$\prod_{s=1}^{p} \text{mcd}\,(f(x), g(x) - s) \mid f(x),$$

ya que todos los mcd de la izquierda son divisores de $f(x)$ (evidentemente) y, como los $g(x) - s$ son primos entre sí, también lo son los mcd.

En el otro sentido, si tomamos un factor irreducible de $f(x)$, pongamos $h(x)$, debe dividir a $g(x)^p - g(x)$, luego divide a alguno de los $g(x) - s$ y, por tanto, al mcd $(f(x), g(x) - s)$ correspondiente.

Por tanto, los dos miembros de la igualdad se dividen mutuamente y, al no tener factores repetidos y ser mónicos, eso implica la igualdad. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– A partir de aquí, la factorización de $f(x) \in \mathbf{Z}/\mathbf{Z}p[x]$ queda reducida, por un lado, a encontrar $g(x)$ (que podemos suponer de grado r, menor que n) tal que

$$f(x) \mid (g(x)^p - g(x)),$$

y posteriormente a aplicar el algoritmo de Euclides. Notemos entonces que, por estar en característica p y por el Pequeño Teorema de Fermat,

$$g(x) = \sum_{i=0}^{n-1} a_i x^i \implies g^p(x) = \sum_{i=0}^{n-1} a_i x^{ip}.$$

Vamos entonces a buscar un tal polinomio $g(x)$ (o sea, vamos a buscar los coeficientes $a_0, ..., a_{n-1}$). Dividamos entonces los monomios x^{ip} entre $f(x)$ y, al tener grado n, obtendremos

$$\begin{aligned}
x^{0p} = q_0 f(x) + r_0(x) &= q_0 f(x) + r_{00} + r_{10}x^1 + ... + r_{n-1,0}x^{n-1} \\
x^{1p} = q_1 f(x) + r_1(x) &= q_1 f(x) + r_{01} + r_{11}x^1 + ... + r_{n-1,1}x^{n-1} \\
&\vdots \\
x^{(n-1)p} = q_{n-1} f(x) + r_{n-1}(x) &= q_{n-1} f(x) + r_{0,n-1} + r_{1,n-1}x^1 + ... + r_{n-1,n-1}x^{n-1}
\end{aligned}$$

Por la unicidad de la división euclídea, el resto de dividir $g^p(x)$ entre $f(x)$ es el dado por la expresión

$$g^p(x) = \sum_{i=0}^{n-1} a_i x^{ip} = \left(\sum_{i=0}^{n-1} a_i q_i\right) f(x) + \sum_{i=0}^{n-1} a_i r_i,$$

y por el mismo motivo el resto de dividir $g^p(x) - g(x)$ entre $f(x)$ es el dado por la expresión

$$g^p(x) - g(x) = \sum_{i=0}^{n-1} a_i x^{ip} - \sum_{i=0}^{n-1} a_i x^i = \left(\sum_{i=0}^{n-1} a_i q_i\right) f(x) + \sum_{i=0}^{n-1} (a_i r_i - a_i x_i).$$

Así pues $g(x)$ verifica lo que queremos si y sólo si

$$0 = \sum_{i=0}^{n-1} (a_i r_i - a_i x_i),$$

o, escrito en forma matricial, si llamamos $R = (r_{ij})$, que es una matriz $n \times n$, si y sólo si

$$(a_0, ..., a_{n-1}) \text{ es solución del sistema } (R - I_n) X^t = 0_{n\times 1}.$$

Así, gracias al algoritmo de Berlekamp, factorizar en $\mathbf{Z}/\mathbf{Z}p[x]$ se reduce a resolver sistemas de ecuaciones lineales y aplicar el algoritmo de Euclides, operaciones ambas que se pueden realizar de manera muy eficiente.

Tema 4. Grupos.

Comenzaremos recordando el concepto de grupo, que ya vimos en el Tema 1 y, a continuación, estudiaremos con más detalle esta estructura.

4.1. Grupos: Definiciones y ejemplos.

Definición.– Una *operación interna y binaria* en un conjunto A es una aplicación $\alpha\colon A \times A \to A$.

Observación.– En un lenguaje más coloquial, una operación interna y binaria en A es una regla que asocia a cada par ordenado (a, b) de elementos de A otro elemento de A, $\alpha(a, b)$.

Normalmente, si $\alpha\colon A \times A \to A$ es una operación interna y binaria en A, es costumbre elegir algún símbolo (por ejemplo $\star$) para notar

$$a \star b := \alpha(a, b).$$

Observación.– Para estudiar un conjunto A con "pocos" elementos dotado de una operación binaria $\star$, podemos trabajar con la *tabla de la operación*. Esta tabla es un cuadro de doble entrada en el que se colocan los elementos de A en la línea horizontal de arriba y vertical de la izquierda. En cada casilla libre correspondiente al par ordenado $(a, b) \in A \times A$ se coloca el elemento $a \star b$. Por ejemplo, si $A = \{a, b\}$ y la operación viene determinada por $a \star a = a$, $a \star b = b$, $b \star a = b$ y $b \star b = a$, la tabla será:

$\star$	a	b
a	a	b
b	b	a

Ejemplos.– Algunas opearciones binarias internas bien conocidas.

1. Si a_0 es un elemento fijo de un conjunto A, la aplicación $(a, b) \in A \times A \mapsto a_0$ es una operación interna y binaria constante.

2. La suma y el producto usuales son operaciones internas y binarias en los conjuntos de números $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ y $\mathbf{Z}/\mathbf{Z}n$, así como en los polinomios con coeficientes en estos conjuntos.

3. La suma es una operación interna y binaria en el conjunto de los vectores $\mathbf{R}^n$ o de las matrices $m \times n$ de números.

4. Cualquier función de dos variables reales $f\colon \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ define una operación interna y binaria en $\mathbf{R}$.

5. Dado un número natural $n \geq 1$, consideremos el conjunto $\mathcal{Z}_n = \{0, 1, \ldots, n-1\}$ y en él la operación interna y binaria cuya tabla es:

$\star$	0	1	2	$\cdots$	$n-2$	$n-1$
0	0	1	2	$\cdots$	$n-2$	$n-1$
1	1	2	3	$\cdots$	$n-1$	0
2	2	3	4	$\cdots$	0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$n-2$	$n-2$	$n-1$	0	$\cdots$	$n-4$	$n-3$
$n-1$	$n-1$	0	1	$\cdots$	$n-3$	$n-2$

6. Dado un conjunto X, consideremos el conjunto $\mathcal{A}_X$ de las aplicaciones de X en sí mismo. La composición de aplicaciones es una operación interna y binaria en $\mathcal{A}_X$.

7. Dado un conjunto X, la unión y la intersección con operaciones internas y binarias en $\mathcal{P}(X)$.

Observación.– En lo que sigue, "operación en A" significa "operación interna y binaria en A."

Definición.– Dada una operación $\star$ sobre un conjunto A, diremos que:

1. Es *conmutativa* si $a \star b = b \star a$ para todo $a, b \in A$.

2. Es *asociativa* si $a \star (b \star c) = (a \star b) \star c$ para todo $a, b, c \in A$.

3. El elemento $e \in A$ es *elemento neutro* si $e \star a = a \star e = a$ para todo $a \in A$.

Proposición.– Si una operación en A tiene elemento neutro, éste es único.

Demostración.– Sea un conjunto A con una operación binaria $\star$. Sean $e \in A$ un elemento neutro a la izquierda y $e' \in A$ un elemento neutro a la derecha. Por ser e elemento neutro a la izquierda se tiene

$$e \star e' = e',$$

por ser e' elemento neutro a la derecha se tiene

$$e \star e' = e.$$

De donde $e = e'$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Dado un conjunto A dotado de una operación $\star$ con un elemento neutro e, y dado un elemento $x \in A$, diremos que x' es *simétrico* de x si $x' \star x = x \star x' = e$.

Proposición.– En las condiciones de la definición anterior, se tiene lo siguiente:

1. Si la operación $\star$ es asociativa, x' es simétrico de x e y' es simétrico de y, entonces $y' \star x'$ es simétrico de $x \star y$.

2. Si la operación $\star$ es asociativa, entonces el simétrico de un elemento, si existe, es único.

Demostración.– Para probar 2, supongamos que x' y x'' son simétricos de x, entonces, usando la asociatividad,

$$x'' = (x' \star x) \star x'' = x' \star (x \star x'') = x'.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Un grupo es un par $(G, \star)$, donde G es un conjunto y $\star$ es una operación interna y binaria sobre G verificando las siguentes propiedades:

1. La operación es asociativa.
2. La operación tiene elemento neutro.
3. Cada elemento de G posee un simétrico.

Si además la operación es conmutativa entonces se dice que el grupo es *abeliano* o *conmutativo*.

Ejemplos.– Algunos grupos bien conocidos

1. $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ y $\mathbf{Z}/\mathbf{Z}n$ son grupos abelianos con la adición.
2. $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$, $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ y $\mathbf{C}^* = \mathbf{C} \setminus \{0\}$ son grupos abelianos con la multiplicación.
3. Si p es primo $(\mathbf{Z}/\mathbf{Z}p)^*$ es grupo abeliano con la multiplicación.
4. El conjunto S_A de las biyecciones de A en A es un grupo con la composición. Si A tiene más de 2 elementos, S_A no es abeliano. Si $A = \{1, \ldots, n\}$, se nota indistintamente S_n o S_A.
5. El conjunto de las funciones (continuas, diferenciables,...) definidas en un abierto de $\mathbf{R}$ con valores reales, con la suma *"punto a punto"*, es un grupo abeliano.
6. El conjunto de las matrices $n \times n$, con elementos en un cuerpo k y determinante no nulo, $\mathrm{GL}(n, k)$, es un grupo (no abeliano si $n \geq 2$) con la multiplicación de matrices.

Observación.– Cuando usemos la notación aditiva o la multiplicativa, el elemento neutro y el simétrico de x serán notados de la siguiente forma:

	elemento neutro	elemento simétrico de x
$+$	0	$-x$ (opuesto de x)
$\cdot$	1	x^{-1} (inverso de x)

4.2. Subgrupos.

Definición.– Sea $(G, \star)$ un grupo. Un subconjunto no vacío H de G se dice que es un subgrupo de $(G, \star)$ si $(H, \star)$ es un grupo. Es decir, que efectivamente un subgrupo es un grupo dentro de otro grupo con la misma operación.

Proposición.– Sean $(G, \star)$ un grupo y $H \subset G$ un subconjunto no vacío. Las condiciones siguientes son equivalentes:

1. H es un subgrupo de $(G, \star)$.
2. $\forall x, y \in H, x \star y' \in H$.

Demostración.– Veamos primero $1 \Rightarrow 2$. Supongamos que H es un subgrupo y sean $x, y \in H$. Como H es subgrupo contiene los simétricos de todos sus elementos, en particular $y' \in H$. De nuevo como H es subgrupo, $\star$ es una operación interna, de donde $x \cdot y' \in H$, como queríamos.

Probemos ahora $2 \Rightarrow 1$: Como $H \subset G$, los elementos de H verifican la propiedad asociativa. Como H es no vacío, sea $x \in H$. Aplicando 2) obtenemos

$$x \star x' = e \in H.$$

Si $x \in H$, aplicando de nuevo 2) para e y x, tenemos

$$e \star x' = x' \in H,$$

luego H contiene los simétricos de todos sus elementos. Sean $x, y \in H$, aplicando *2)* esta vez para x, y' se tiene

$$x \star (y')' = x \star y \in H. \tag{1}$$

Luego H es subgrupo de $(G, \star)$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– De ahora en adelante si escribimos el *"grupo G"* en lugar de el *"grupo $(G, \star)$"*, sobreentendemos que la operación binaria la notamos con el símbolo $\star$.

Ejemplos.– Algunos subgrupos ya tratados:

1. Para todo grupo G, $\{e\}$ y G son subgrupos de G y se denominan *subgrupos triviales* de G.
2. *Subgrupos de* $(\mathbf{Z}, +)$*:* Dado $n \in \mathbf{Z}$, $n \geq 0$, sea $\mathbf{Z}n = \{k \cdot n \mid k \in \mathbf{Z}\}$. Se tiene:
   (a) $\mathbf{Z}n$ es un subgrupo de $\mathbf{Z}$.
   (b) Todo subgrupo de $\mathbf{Z}$ es de la forma $\mathbf{Z}n$ para algún $n \geq 0$.
3. Raíces n–ésimas de la unidad dentro de $\mathbf{C}^*$.
4. Si $C \subset A$, el conjunto $\{f \in S_A \mid f(a) = a, \ \forall a \in C\}$ es un subgrupo de S_A.

Proposición.– Sean G un grupo, $\{H_i \mid i \in I\}$ una familia de subgrupos de G. Entonces $\cap_{i \in I} H_i$ es un subgrupo de G.

Demostración.– La intersección de subgrupos es no vacía porque el elemento neutro está en todos los subgrupos. Además,

$$x, y \in \bigcap_{i \in I} H_i \Rightarrow x, y \in H_i \; \forall i \in I \Rightarrow x \star y' \in H_i \; \forall i \in I \Rightarrow x \star y' \in \bigcap_{i \in I} H_i.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Dado un subconjunto A de un grupo G, llamamos *subgrupo generado por* A al subgrupo de G:

$$\langle A \rangle = \bigcap \{H \mid H \text{ subgrupo de } G \text{ y } A \subset H\}.$$

Proposición.– Sean G un grupo y $A \subset G$ un subconjunto, entonces $\langle A \rangle$ es el menor subgrupo de G que contiene a A.

Demostración.– Es inmediato de la definición de $\langle A \rangle$: Si H es un subgrupo que contiene a A, es evidente que $\langle A \rangle \subset H$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Se dice que $A \subset G$ es un *sistema de generadores* de un grupo G si $G = \langle A \rangle$.

Un caso particular, e importante, de sistema de generadores de un grupo es cuando $A = \{a\}$ posee un sólo elemento. Éstos se estudian en la siguiente sección.

Proposición.– Sean G un grupo y $A \subset G$ un subconjunto. Sea $A' = \{x' \mid x \in A\}$. Entonces

$$\langle A \rangle = \{x_1 \star x_2 \star \ldots \star x_n \mid x_i \in A \cup A', n \geq 1\}.$$

Demostración.– Es evidente que

$$\langle A \rangle \supset \{x_1 \star x_2 \star \ldots \star x_n \mid x_i \in A \cup A', n \geq 1\}.$$

Para la otra inclusión usaremos que $\langle A \rangle$ es el menor subgrupo que contiene a A. Se comprueba fácilmente que $A \subset \{x_1 \star x_2 \star \ldots \star x_n \mid x_i \in A \cup A', n \geq 1\}$ y que $\{x_1 \star x_2 \star \ldots \star x_n \mid x_i \in A \cup A', n \geq 1\}$ es un subgrupo. De donde

$$\langle A \rangle \subset \{x_1 \star x_2 \star \ldots \star x_n \mid x_i \in A \cup A', n \geq 1\}.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

4.3. Grupos cíclicos.

Definición.– Sea $(G, \star)$ un grupo. Definimos

$$a^m = \begin{cases} e & \text{si} \quad m = 0 \\ \overset{(m \text{ veces})}{a \star \ldots \star a} & \text{si} \quad m > 0 \\ \overset{(m \text{ veces})}{a' \star \ldots \star a'} & \text{si} \quad m < 0 \end{cases}$$

Si G es un grupo cuya operación se nota *multiplicativamente*, entonces

$$a^m = \begin{cases} 1 & \text{si} \quad m = 0 \\ \overset{(m\ veces)}{a \cdot \ldots \cdot a} & \text{si} \quad m > 0 \\ \overset{(m\ veces)}{a^{-1} \cdot \ldots \cdot a^{-1}} & \text{si} \quad m < 0 \end{cases}$$

Si la notación es *aditiva*, entonces

$$ma = \begin{cases} 0 & \text{si} \quad m = 0 \\ \overset{(m\ veces)}{a + \ldots + a} & \text{si} \quad m > 0 \\ \overset{(m\ veces)}{(-a) + \ldots + (-a)} & \text{si} \quad m < 0 \end{cases}$$

Definición.– Se dice que un grupo G es *cíclico* si existe $a \in G$ tal que

$$G = \langle a \rangle = \langle \{a\} \rangle = \{a^m \mid m \in Z\}.$$

La notación habitual para este tipo de grupos, cuando se sobreentiende la operación es C_n (cuando G tiene n elementos) o C_∞ (cuando tiene infinitos elementos).

Observación.– Si G es un grupo cíclico entonces G es abeliano.

Proposición.– Todo subgrupo de un grupo cíclico es cíclico.

Demostración.– Sea $H \subset G = \langle a \rangle$ un subgrupo. Sea $s = \min\{k > 0 \mid a^k \in H\}$. Veamos que $H = \langle a^s \rangle$ por doble inclusión.

Como $a^s \in H$, entonces $\langle a^s \rangle \subset H$. En otro sentido, sea $h \in H$. Como $h \in G$, $h = a^m$, para algún entero positivo m. (En caso contrario razonaríamos con h'.)

Por el algoritmo de la división tenemos $m = qs + r$, con $0 \leq r < l$. Entonces $a^m = (a^s)^q \star a^r$, de donde $a^r \in H$. Como s es el menor entero no nulo con esa propiedad ha de ser $r = 0$, y $a^m = (a^s)^q \in \langle a^s \rangle$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Gracias a este resultado podemos estudiar con detalle todos los subgrupos de un grupo cíclico.

Proposición.– Sea $G = \langle a \rangle$ un grupo cíclico finito de orden m.

1. Si H es subgrupo de G, entonces H es cíclico o $H = \{1\}$. Si $H = \langle a^l \rangle$, con $l = \min\{k | a^k \in H\}$ entonces l divide a m y $|H| = m/l$.
2. Si k divide a m entonces $K = \langle a^k \rangle$ es de orden m/k.
3. El número de subgrupos distintos de G es el mismo que el número de divisores distintos de m.
4. Existe a lo sumo un subgrupo de G de cualquier orden dado.

Demostración.– El primer apartado ya lo hemos demostrado, esencialmente, en la proposición anterior. En cuanto al segundo, notemos que, en las condiciones del enunciado, si llamamos $p = m/k$,

$$K = \left\{1, a^k, a^{2k}, ..., a^{(p-1)k}\right\}.$$

Así, para cada d, divisor de m tenemos exactamente un subgrupo de G (de orden m/d), lo que demuestra el resultado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Proposición.– Sea $G = \langle a \rangle$ un grupo cíclico infinito. Entonces para cada $n \geq 2$ existe un único subgrupo (no trivial) de G.

Demostración.– Dado que todos los subgrupos son cíclicos, han de ser de la forma $K = \langle a^r \rangle$, con $r \in \mathbf{Z}$. Basta observar entonces que, por un lado

$$\langle a^r \rangle = \langle a^{-r} \rangle$$

y, por otra parte, si $0 < r < s$ se tiene que $a^r \notin \langle a^s \rangle$, por lo que todos los subgrupos son diferentes. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

4.4. Orden de un elemento de un grupo.

Definición.– Sean G un grupo (no necesariamente cíclico) y $a \in G$. Diremos que

1. a tiene *orden infinito* si todas las potencias de a son distintas entre sí.
2. a tiene *orden finito* si existen $0 \leq m < n$ tales que $a^n = a^m$.

Ejemplos.– Obviamente todo elemento de un grupo finito ha de tener orden finito. En grupos infinitos podemos tener tanto órdenes finitos como infinitos.

1. Sea $a \in \mathbf{Z}$, $a \neq 0$. Entonces a tiene orden infinito.
2. El elemento
$$A = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \in \mathrm{GL}(2, \mathbf{C})$$
tiene orden finito. Notemos que el grupo es, en este caso, infinito.

Proposición.– Sean G un grupo y $a \in G$. Consideremos el subgrupo $\langle a \rangle$.

1. Si a es de orden infinito, entonces
   (a) $a^n = e \Leftrightarrow n = 0$.
   (b) La aplicación $\varphi\colon \mathbf{Z} \to \langle a \rangle$ dada por $\varphi(n) = a^n$ es biyectiva.
   (c) $\langle a \rangle$ es un grupo infinito.
2. Si a es de orden finito, entones
   (a) Existe $n > 0$ tal que $a^n = e$.

(b) Sea m el menor entero estrictamente positivo tal que $a^m = 1$. Entonces los a^i, $0 \geq i \geq m-1$ son distintos entre sí y

$$\langle a \rangle = \{1, a, a^2, \ldots, a^{m-1}\}.$$

Demostración.– Casi todas las afirmaciones son directas.

1. Si a es de orden infinito, las propiedades a), b) y c) se prueban fácilmente.
2. Supongamos que a tiene orden finito.

   (a) Si a tiene orden finito existen dos enteros $0 \leq k < l$ tales que $a^k = a^l$. Sea $n = l - k$, entonces

   $$a^n = a^{l-k} = a^l \star a^{-k} = a^l \star a'^k \overset{a^l = a^k}{=} a^k \star a'^k = e. \tag{2}$$

   (b) Sea $m > 0$ el menor tal que $a^m = 1$. Sean $0 \leq i \leq j \leq m-1$ dos enteros tales que $a^i = a^j$, es decir, tales que $a^{j-i} = 1$. Como $j - i < m$, debe ser $j - i = 0$, es decir, $i = j$. Luego todos los a^i, $0 \leq i \leq m-1$ son distintos.

   Es evidente que $\langle a \rangle \supset \{1, a, a^2, \ldots, a^{m-1}\}$. Sea a^n un elemento cualquiera de $\langle a \rangle$, escribamos $n = q \cdot m + r$, $0 \leq r \leq m-1$, la división euclídea de n entre m, entonces

   $$a^n = a^{q \cdot m + r} = a^{q \cdot m} \star a^r = (a^m)^q \star a^r = a^r. \tag{3}$$

   Luego $\langle a \rangle \subset \{1, a, a^2, \ldots, a^{m-1}\}$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Sean G un grupo y $a \in G$ de orden finito. El *orden* de a, notado por $o(a)$, es el menor entero estrictamente positivo, m, tal que $a^m = e$.

Proposición.– Sean G un grupo y $a \in G$. Se tienen las siguientes propiedades:

1. $o(a) = 1 \Longleftrightarrow a = e$.
2. Si $a \in G$ tiene orden finito, entonces $o(a) = o(a')$.
3. Si $a \in G$ tiene orden infinito, a' tiene orden infinito.
4. Si G es finito, todo elemento de G tiene orden finito.
5. Si $o(a) = m$ y $a^n = e$, entonces $m \mid n$.

Demostración.– Los primeros cuatro apartados se obtienen inmediatamente de las definiciones. Para el apartado 5) basta realizar la división euclídea de n entre m, obteniendo $n = q \cdot m + r$, con $0 \leq r \leq m-1$, de donde

$$e = a^n = a^{q \cdot m + r} = a^{q \cdot m} \star a^r = (a^m)^q \star a^r = a^r.$$

Como m es el menor estrictamente positivo tal que $a^m = e$, debe ser $r = 0$ y, por tanto, $m \mid n$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– El siguiente resultado nos da el orden de todos los elementos de un grupo cíclico finito.

Proposición.– Sea $G = \langle a \rangle = C_n$ un grupo cíclico de orden finito n. Entonces, $\forall m, 0 \leq m < n$, se verifica que

$$o(a^m) = \frac{n}{\text{mcd}(n, m)}.$$

Demostración.– Sea

$$d = \text{mcd}(m, n), \quad m = m'd, \quad n = n'd.$$

En primer lugar tenemos que $(a^m)^{n'} = a^{mn'} = (a^n)^{m'} = e$. Supongamos que $(a^m)^t = a^{mt} = e$. Por definición de orden es $n \mid mt$, es decir $mt = nk$. Dividiendo por d,

$$m't = n'k \implies n' \mid m't.$$

Como m' y n' son primos entre sí, es $n' \mid t$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

4.5. Teorema de Lagrange

Definición.– Sean G un grupo y $H \subset G$ un subgrupo. Sobre G definimos las relaciones $\sim_H$ y ${}_H\sim$ de la manera siguiente: Dados $x, y \in G$,

$$x \sim_H y \Leftrightarrow x' \star y \in H \qquad x \,{}_H\!\sim y \Leftrightarrow y \star x' \in H.$$

Proposición.– En las condiciones de la definición anterior, las relaciones $\sim_H$ y ${}_H\sim$ son relaciones de equivalencia.

Demostración.– Se comprueba que ambas relaciones verifican las propiedades:

1. Reflexiva: $\forall x \in G,\ x \sim x$.
2. Simétrica: $\forall x, y \in G,\ x \sim y \Rightarrow y \sim x$.
3. Transitiva: $\forall x, y, z \in G,\ x \sim y, y \sim z \Rightarrow x \sim z$.

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Proposición.– Sean G un grupo y $a \in G$. Consideremos los conjuntos

$$a \star H = \{a \star h \mid h \in H\}, \qquad H \star a = \{h \star a \mid h \in H\}.$$

Se tiene:

1. $a \star H$ es la clase de equivalencia de a para la relación $\sim_H$.
2. $H \star a$ es la clase de equivalencia de a para la relación ${}_H\sim$.

Demostración.– Basta probar el primer apartado, pues el segundo es análogo. Sea $a \in G$ y llamemos $\bar{a}$ a su clase de equivalencia por $\sim_H$, es decir,

$$\bar{a} = \{b \in G \mid a \sim_H b\} = \{b \in G \mid a' \star b \in H\}.$$

Probaremos por doble inclusión que $\bar{a} = a \cdot H$. Si $b \in \bar{a}$, entonces $a' \star b \in H$, es decir, existe $h \in H$ tal que $a' \star b = h$, de donde

$$b = a \star h \in a \star H.$$

Si $b \in a \star H$, existe $h \in H$ tal que $b = a \star h$, de donde

$$a' \star b = h \in H \Rightarrow a \sim_H b.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Proposición.- Si G es un grupo abeliano, entonces $\sim_H$ y ${}_H\sim$ coinciden.

Sean G un grupo y H un subgrupo, notaremos

$$G\colon H = \frac{G}{\sim_H}, \qquad H\colon G = \frac{G}{{}_H\sim}.$$

Observación.– Las clases de equivalencia de una relación de equivalencia son una partición del conjunto total, es decir, dadas dos clases de equivalencia, o son disjuntas, o coinciden. En consecuencia, si tomamos $x, y \in G$, tenemos que, o bien $x \star H = y \star H$, o bien $x \star H \cap y \star H = \emptyset$. Análogamente se tiene que, dados $x, y \in G$, o bien $H \star x = H \star y$, o bien $H \star x \cap H \star y = \emptyset$.

Ejemplos.– Algunas relaciones de equivalencia de este tipo.

1. Sea $n \in \mathbf{Z}$, $n > 0$. Se tiene

   $$\mathbf{Z}\colon \mathbf{Z}n = \mathbf{Z}n\colon \mathbf{Z} = \{0 + \mathbf{Z}n, \ldots, (n-1) + \mathbf{Z}n\},$$

   donde las clases anteriores son distintas entre sí.

2. Consideremos el subgrupo $H \subset \mathrm{GL}(2, \mathbf{C})$ dado por

   $$H = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda = 1, -1, i, -i \right\}.$$

   Para todo $A \in \mathrm{GL}(2, \mathbf{C})$, $A \cdot H = H \cdot A$. Por tanto $\sim_H = {}_H\sim$, aún sin ser $\mathrm{GL}(2, \mathbf{C})$ un grupo abeliano.

3. Sea $H \subset \mathrm{GL}(2, \mathbf{C})$ el subgrupo

   $$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \right\}.$$

   Sea la matriz

   $$A = \begin{pmatrix} 3 & 2 \\ 5 & 4 \end{pmatrix},$$

se tiene que:

$$A \cdot H = \left\{ \begin{pmatrix} 3 & 2 \\ 5 & 4 \end{pmatrix}, \begin{pmatrix} 2i & 3i \\ 4i & 5i \end{pmatrix}, \begin{pmatrix} -3 & -2 \\ -5 & -4 \end{pmatrix}, \begin{pmatrix} -2i & -3i \\ -4i & -5i \end{pmatrix} \right\}$$

$$H \cdot A = \left\{ \begin{pmatrix} 3 & 2 \\ 5 & 4 \end{pmatrix}, \begin{pmatrix} 5i & 4i \\ 3i & 2i \end{pmatrix}, \begin{pmatrix} -3 & -2 \\ -5 & -4 \end{pmatrix}, \begin{pmatrix} -5i & -4i \\ -2i & -2i \end{pmatrix} \right\}.$$

Como $A \cdot H \neq H \cdot A$, es ${}_H\sim \neq \sim_H$.

Definición.– Dado un grupo finito G, definimos su *orden*, que notaremos $|G|$, como el cardinal del conjunto G.

Teorema de Lagrange.–. Sea G un grupo finito, $H \subset G$ un subgrupo. Entonces $|H|$ divide a $|G|$.

Demostración.– Consideremos la relación $\sim_H$ sobre G. Como G es finito, habrá sólo un número finito de clases de equivalencia distintas. Sean éstas $a_1 \star H, \ldots, a_r \star H$. Como G es unión disjuntas de estas clases, será

$$|G| = \#(a_1 \star H) + \cdots + \#(a_r \star H).$$

Sea $H = \{h_1, \ldots, h_n\}$, entonces $a_i \star H = \{a_i \star h_1, \ldots, a_i \star h_n\}$, $1 \leq i \leq r$. Veamos que $\#(a_i \star H) = |H|,\ 1 \leq i \leq r$. En efecto, si $a_i \star h_j = a_i \star h_l$ se deduce que, multiplicando a izquierda por el simétrico de a_i, $h_j = h_l$. Por tanto los elementos de la clase $a_i \cdot H$ son todos distintos. Luego $|G| = r \cdot |H|$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Corolario.– Sean G un grupo de orden finito y $H \subset G$ un subgrupo. El número de clases de equivalencia para $\sim_H$ coincide con el número de clases de equivalencia para ${}_H\sim$ y es igual a $|G|/|H|$.

Demostración.– La demostración del teorema de Lagrange podía haberse hecho con la relación ${}_H\sim$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Sean G un grupo y $H \subset G$ un subgrupo. Se llama *índice* de H en G al número de clases de equivalencia para la relación $\sim_H$ (o ${}_H\sim$), es decir, al número

$$i(G : H) = \frac{|G|}{|H|}.$$

Corolario.– Sean G un grupo finito y , $K \subset G$ subgrupos. Se tienen las siguientes propiedades:

1. Para cada $a \in G$ se tiene que $o(a)$ divide a $|G|$.
2. Si el orden de G es primo, entonces G es cíclico y no tiene más subgrupos que los triviales.
3. Si $|H|$ y $|K|$ son primos entre sí, entonces $H \cap K = \{1\}$.

Demostración.– Todos son consecuencias casi inmediatas del Teorema de Lagrange.

1. Sea $a \in G$ y consideremos el subgrupo $\langle a \rangle \subset G$. Sabemos que $o(a) = |\langle a \rangle|$. Por otro lado, el teorema de Lagrange dice que $|\langle a \rangle|$ divide a $|G|$.

2. Sea $a \in G$, $a \neq 1$. El subgrupo $\langle a \rangle \subset G$ no es trivial y su orden divide al número primo $|G|$, luego debe ser $o(a) = |G|$. De donde $G = \langle a \rangle$. Si no existe $a \in G$, $a \neq 1$, entonces $G = \{1\}$ es cíclico.

3. $H \cap K$ es un subgrupo de H y de K, luego $|H \cap K|$ debe dividir a $|H|$ y a $|K|$, que son primos entre sí. De donde $|H \cap K| = 1$ y $H \cap K = \{1\}$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

4.6. Subgrupos normales. Grupo cociente y grupo producto.

Si G es un grupo y H es un subgrupo, hemos visto en el tema anterior que los conjuntos cocientes $G\colon H$ y $H\colon G$ son generalmente distintos y no siempre heredan la estructura de grupo de G. Nos interesa estudiar los subgrupos para los cuales esto no ocurre.

Lema.– Sean $H_1 \subseteq H_2$ subgrupos de un grupo G. Entonces $\forall g, \widetilde{g} \in G$, se verifica que $g \star H_1 \star \widetilde{g} \subseteq g \star H_2 \star \widetilde{g}$.

Proposición.– Sea H un subgrupo de un grupo G. Las condiciones siguientes son equivalentes:

1. Las relaciones $\sim_H$ y ${}_H\sim$ coinciden, es decir, $x \star H = H \star x$ para todo $x \in G$.

2. Para todo $x \in G$, se tiene $\subset H$.

3. Para todo $x \in G$, se tiene $x \star H \star x' = H$.

Demostración.– Seguiremos el esquema $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$.

$1 \Rightarrow 2$ Supongamos que $x \star H = H \star x$ para todo $x \in G$. Sea $x \star h \star x' \in x \star H \star x'$. Como $x \star h \in x \star H = H \star x$, se tiene que $\exists \widetilde{h} \in H$ tal que $x \star h = \widetilde{h} \star x$. Entonces $x \star h \star x' = \widetilde{h} \star x \star x' = \widetilde{h} \in H$.

$2 \Rightarrow 3$ Supongamos que, para todo $x \in G$, $x \star H \star x' \subset H$. Por el lema tenemos que $x' \star x \star H \star x' \star x \subset x' \star H \star x$, $\forall x \in G$, y por tanto $x \star H \star x' = H$.

$3 \Rightarrow 1$ Supongamos por último que para todo $x \in G$ se tiene $x \star H \star x' = H$. Por el lema tenemos que $x \star H = x \star H \star x' \star x = H \star x$.

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Un subgrupo H de G se dice *normal* en G si satisface alguna de las condiciones anteriores, y lo notaremos $H \lhd G$.

Proposición.– Sea H es un subgrupo normal de G, el conjunto cociente $G\colon H = H\colon G$, que notaremos G/H, es un grupo con la operación inducida por la de G.

Demostración.– El producto de clases se define de la siguiente manera:

$$(x \star H) \star (y \star H) = (x \star y) \star H, \forall x, y \in G.$$

Veamos que esta operación está bien definida, es decir, no depende del representante elegido. En efecto, sean $x \star H = \widetilde{x} \star H, y \star H = \widetilde{y} \star H$, tenemos que probar que $(x \star y) \star H = (\widetilde{x} \star \widetilde{y}) \star H$, o, equivalentemente, que $x' \star y' \star \widetilde{x} \star \widetilde{y} \in H$. Como $y' \star \widetilde{y} \in H$, es

$$x' \star y' \star \widetilde{y} \in x' \star H = \widetilde{x}' \star H = H \star \widetilde{x}'.$$

Luego, multiplicando por $\widetilde{x}$ a la derecha se tiene que

$$x' \star y' \star \widetilde{x} \star \widetilde{y} \in H.$$

El neutro es $e \star H = H$, y el simétrico de $x \star H$ es $x' \star H$. Además G/H será abeliano si G lo es.

Ejemplos.– Algunos grupos normales y no normales.

1. $\{1\} \lhd G$.
2. Todos los subgrupos de un grupo abeliano.
3. El conjunto de todas las matrices diagonales regulares es un subgrupo *no normal* del grupo lineal $\mathrm{GL}(n, \mathbf{Q})$.
4. El conjunto de las matrices escalares λI, con $\lambda \in \mathbf{Q}$, es un subgrupo normal del grupo lineal $\mathrm{GL}(n, \mathbf{Q})$.

Observación.– A diferencia de la operación cociente, la operación de producto de grupos es mucho más natural y sencilla.

Definición.– Sean $(G_1, \star_1), \ldots, (G_n, \star_n)$ grupos. En el conjunto $G_1 \times \cdots \times G_n$ definimos la siguiente operación binaria:

$$(a_1, \ldots, a_n) \star (b_1, \ldots, b_n) = (a_1 \star_1 b_1, \ldots, a_n \star_n b_n).$$

Proposición.– $(G_1 \times \cdots \times G_n, \star)$ es un grupo.

Demostración.– Se verifican las propiedades de manera casi directa:

1. La operación $\star$ es asociativa por serlo cada una de las operaciones $\star_i$, $i = 1, \ldots, n$.
2. Si e_i es el elemento neutro del grupo $(G_i, \star_i)$, con $i = 1, \ldots, n$, entonces $(e_1, \ldots, e_n)$ es el elemento neutro de $(G_1 \times \cdots \times G_n, \star)$.
3. El simétrico de un elemento $(a_1, \ldots, a_n) \in G_1 \times \cdots \times G_n$ es $(a_1', \ldots, a_n')$, donde cada a_i' es el simétrico de a_i en el grupo $(G_i, \star_i)$, con $i = 1, \ldots, n$.

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Proposición.– En las condiciones anteriores, $(G_1 \times \cdots \times G_n, \star)$ es abeliano si y sólo si cada $(G_i, \star_i)$, con $i = 1, \ldots, n$, lo es.

Demostración.– Es inmediato. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Proposición.– Dados dos grupos cíclicos C_n y C_m, se tiene que $C_n \times C_m$ es cíclico si y sólo si mcd(n, m)=1

Demostración.– Supongamos, en primer lugar, $C_n = \langle a \rangle$ y $C_m = \langle b \rangle$ siendo n y m primos entre sí y notaremos 1 el elemento neutro en ambos grupos. Consideramos entonces $(a, b) \in C_n \times C_m$. Entonces tenemos que

$$(a,b)^r = (1,1) \implies a^r = 1,\ b^r = 1 \implies n|r,\ m|r$$

y, por ser entones mcd$(n, m) = 1$, ha de ser $nm|r$. Como $(a, b)^{nm} = 1$ concluimos que $C_n \times C_m = \langle (a, b) \rangle$.

En el otro sentido, supondremos que mcd$(n, m) = d > 1$. Entonces es sencillo comprobar que, para cualesquiera $r, s \in \mathbf{N}$,

$$(a^r, b^s)^{nm/d} = \left(a^{n(rm/d)}, b^{m(sn/d)}\right) = (1,1),$$

luego ningún elemento tiene orden nm y el grupo producto no es cíclico. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

4.7. Homomorfismos de grupos.

Cuando definimos aplicaciones entre grupos, nos interesan especialmente aquéllas que conservan las operaciones. Éstas son los homomorfismos de grupos.

Definición.– Sean $(G, \star)$ y $(S, \bullet)$ dos grupos, de elementos neutros e_G y e_S, donde notaremos por g' el inverso de g si $g \in G$, y por $\widetilde{s}$ si $s \in S$.

Un *homomorfismo de grupos* de G en S es una aplicación $f\colon G \to S$ tal que

$$f(x \star y) = f(x) \bullet f(y)$$

para cualesquiera $x, y \in G$.

Algunos tipos especiales de homomorfismos son:

1. Cuando $G = S$, f se dice un endomorfismo.
2. Llamamos *monomorfismos* a los homomorfismos inyectivos y *epimorfismos* a los homomorfismos sobreyectivos de grupos.
3. Cuando $f : G \longrightarrow S$ es biyectivo, se dice un isomorfismo.
4. Cuando f es un endomorfismo biyectivo de G, se dice un automorfismo de G.

Proposición.– Si $f\colon G \longrightarrow S$ es un homomorfismo, se tiene que $f(e_G) = e_S$ y que $f(x') = \widetilde{f(x)}, \forall x \in G$.

Demostración.– Para ver la primera propiedad, tomamos $s \in S$ cualquiera, pero tal que exista $g \in G$ con $f(g) = s$. Entonces

$$f(e_G) \bullet s = f(e_G) \bullet f(g) = f(e_G \star g) = f(g) = s \implies f(e_G) = s \bullet \widetilde{s} = e_S.$$

La otra propiedad se deduce inmediatamente de ésta. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Ejemplos.– Algunos homomorfismo de grupos sencillos.

1. La aplicación constante $f\colon G \longrightarrow S$, $f(x) = e_S\ \forall x \in G$, es un homomorfismo.
2. Sea G un grupo y $x \in G$. La aplicación $i_x\colon G \to G$, $i_x(y) = x \star y \star x'$ es un homomorfismo. Además i_x es biyectiva y $(i_x)^{-1} = i_{x'}$.
3. Si $H \subset G$ es un subgrupo, la inclusión de H en G es un homomorfismo inyectivo.
4. Si $H \triangleleft G$, la proyección canónica $\pi\colon G \to G/H$, $\pi(x) = x\star H$, es un homomorfismo sobreyectivo de grupos.

Observación.– El conjunto de los automorfismos de un grupo G, $\mathrm{Aut}(G)$, es un grupo con la composición de aplicaciones. La aplicación $i\colon G \longmapsto \mathrm{Aut}(G)$ definida por $i(x) = i_x$, para cada $x \in G$, es también un homomorfismo de grupos.

Proposición.– Sea $f\colon G \longrightarrow S$ un homomorfismo de grupos:

1. Si $H \subset G$ es un subgrupo, $f(H)$ es un subgrupo de S. En particular, la imagen $\mathrm{Im}(f) = \{f(g) \mid g \in G\}$ es un subgrupo de S.
2. Si $T \subset S$ es un subgrupo (normal), $f^{-1}(T)$ es un subgrupo (normal) de G. En particular, el núcleo de f,
$$\ker(f) = f^{-1}\left(\{e_S\}\right),$$
es un subgrupo normal de G.
3. f es un monomorfismo si y sólo si $\ker(f) = \{e_G\}$.

Demostración.– Fijamos $f\colon G \longrightarrow S$ y las notaciones anteriores.

1. $f(H) = \{s \in S \mid \exists x \in G \text{ tal que } f(x) = s\}$. Como $e_S = f(e_G) \in f(H)$, $f(H)$ es no vacío. Sean $s, t \in f(H)$, sean $x, y \in H$ tales que $f(x) = s$ y $f(y) = t$. Entonces
$$s \bullet \widetilde{t} = f(x) \bullet \widetilde{f(y)} = f(x) \bullet f(y') = f(x \star y') \in f(H)$$
pues, por ser H subgrupo, $x \star y' \in H$.
2. La prueba de que
$$f^{-1}(T) = \{x \in G \mid f(x) \in T\}$$
es un subgrupo de G es análoga a la del apartado anterior. Veamos que si $T \triangleleft S$ entonces $f^{-1}(T) \triangleleft G$. Basta demostrar que
$$x \star f^{-1}(T) \star x' \subset f^{-1}(T)\ \forall x \in G.$$
Sea $x \star y \star x' \in x \star f^{-1}(T) \star x'$, con $f(y) \in T$. Entonces
$$f(x \star y \star x') = f(x) \bullet f(y) \bullet \widetilde{f(x)} \in f(x) \star T \star \widetilde{f(x)} \subset T$$
por ser $T \triangleleft S$. De donde $x \star y \star x' \in f^{-1}(T)$ y $f^{-1}(T) \triangleleft G$.

3. Supongamos en primer lugar que f es inyectiva, es decir, si $f(x) = f(y)$ entonces $x = y$. Sea $x \in \ker(f)$, entonces

$$f(x) = e_S = f(e_G),$$

de donde $x = e_G$ y $\ker(f) = \{e_G\}$.

Supongamos ahora que $\ker(f) = \{e_G\}$ y sean $x, y \in G$ tales que $f(x) = f(y)$, entonces:

$$f(x) = f(y) \implies e_S = f(x) \bullet \widetilde{f(y)} = f(x \star y') \implies$$

$$\implies x \star y' \in \ker(f) = \{e_G\} \implies x \star y' = e_G \implies x = y.$$

Luego f es inyectiva.

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– El núcleo del homomorfismo $i: G \to \mathrm{Aut}(G)$ es el conjunto $C(G)$ de los elementos de G que conmutan con todos los demás elementos de G, llamado *centro* de G.

4.8. Teoremas de isomorfía

Observación.– Por conveniencia, notaremos a partir de ahora la composición de homomorfismos por simple yuxtaposición. Es un ejercicio sencillo comprobar que, si

$$G \xrightarrow{f} S \xrightarrow{g} X$$

son homomorfismos de grupos, $gf : G \longmapsto X$ también lo es.

Lema.– Sean $f: G \longrightarrow S$ un homomorfismo de grupos y $H \triangleleft G$ tal que $H \subset ker(f)$. Existe un único homomorfismo $f': G/H \longrightarrow G'$ tal que $f = f'\pi$, donde π es la proyección canónica que lleva x en $x \star H$.

Demostración.– Sea la aplicación

$$\begin{array}{rcl} f' : G/H & \longrightarrow & S \\ x \star H & \longmapsto & f'(x \star H) = f(x) \end{array}$$

Veamos que está bien definida, es decir, si tomamos $y \in G$ tal que $y \star H = x \star H$, entonces $f'(y \star H) = f'(x \star H)$. Por definición, $f'(y \star H) = f(y)$ y $f'(x \star H) = f(x)$, luego nos preguntamos si, en estas condiciones, $f(y) = f(x)$. Sabemos, por ser $H \triangleleft G$, que

$$y \star H = x \star H \Leftrightarrow x' \star y \in H \subset ker(f).$$

De donde $e_S = f(x' \star y) = \widetilde{f(x)} \bullet f(y)$ y, por tanto, $f(y) = f(x)$.

Comprobemos ahora que f' es homomorfismo:

$$f'((x \star H) \star (y \star H)) = f'((x \star y) \star H) = f(x \star y) = f(x) \bullet f(y) = f'(x \star H) \bullet f'(y \star H).$$

Falta ver que es único. Sea $g : G/H \longmapsto S$ tal que $f = g\pi$. Entonces, para todo $x \in G$,

$$f'(x \star H) = f(x) = g\pi(x) = g(\pi(x)) = g(x \star H).$$

Luego $f' = g$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Primer teorema de isomorfía.– Sea $f\colon G \longrightarrow S$ un homomorfismo de grupos. Se induce de modo natural un isomorfismo

$$\overline{f} : G/\ker(f) \longrightarrow \mathrm{Im}(f)$$

que factoriza $f = i\,\overline{f}\,\pi$, siendo π el epimorfismo de G sobre $G/\ker(f)$ e i la inclusión de $\mathrm{Im}(f)$ en S.

Demostración.– Basta definir $\overline{f}$ como se definió f' en el lema anterior.

$$\begin{array}{rcl} \overline{f} : G/\ker(f) & \longrightarrow & \mathrm{Im}(f) \\ x \star \ker(f) & \longmapsto & \overline{f}(x \star \ker(f)) = f(x) \end{array}$$

De igual manera que en el lema anterior, se comprueba que $\overline{f}$ está bien definida y que es un homomorfismo.

Sea $x \in G$ tal que $\overline{f}(x \star \ker(f)) = e_S$, es decir, sea $x \star \ker(f) \in \ker(\overline{f})$. Entonces

$$e_S = \overline{f}(x \star \ker(f)) = f(x) \implies x \in \ker(f) \implies x \star \ker(f) = e_G \star \ker(f).$$

Luego $\ker(\overline{f}) = e_G \star \ker(f)$ y $\overline{f}$ es inyectiva.

Por otro lado, si $s \in \mathrm{Im}(f)$, existe $x \in G$ tal que $f(x) = s$, luego $\overline{f}(x \star \ker(f)) = s$ y $\overline{f}$ es sobreyectiva. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Segundo teorema de isomorfía.– Sea $f\colon G \longrightarrow S$ un homomorfismo sobreyectivo de grupos. Sea $J \lhd S$ y pongamos $H = f^{-1}(J)$. Entonces f induce un isomorfismo de G/H en S/J.

Demostración.– Sea π la proyección de S en S/J, que es un homorfismo sobreyectivo. Luego la composición $\pi\, f$ es un homomorfismo sobreyectivo de G en S/J.

Sea $x \in G$ tal que $\pi\, f(x) = e_S \bullet J$, es decir, $x \in ker(\pi\, f)$. Entonces

$$e_S \bullet J = \pi\, f(x) = \pi(f(x)) = f(x) \bullet J \iff f(x) \in J \iff x \in H.$$

Luego $\ker(\pi\, f) = H$ y, aplicando el *primer teorema de isomorfía*, se tiene un isomorfismo de G/H en S/J. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Corolario.– Si H_1 y H_2 son subgrupos normales de G tales que $H_1 \subset H_2$, se tiene:

1. H_2/H_1 es un subgrupo normal de G/H_1.
2. $(G/H_1)/(H_2/H_1)$ es isomorfo a G/H_2.

Demostración.– Veamos ambos enunciados por separado.

1. Primero hemos de ver que $H_1 \lhd H_2$. Sea $x \in H_2 \subset G$, como $H_1 \lhd G$, se tiene $x \star H_1 = H_1 \star x$. de donde $H_1 \lhd H_2$.

Luego podemos considerar el cociente H_2/H_1, que es un subgrupo de G/H_1. Consideremos entonces

$$(x \star H_1) \star (y \star H_1) \star (x' \star H_1) \in (x \star H_1) \star (H_2/H_1) \star (x' \star H_1)\,,$$

con $x \in G$ e $y \in H_2$ arbitarios. Por ser $H_1 \lhd G$, se tiene

$$(x \star H_1) \star (y \star H_1) \star (x' \star H_1) = (x \star y \star x') \star H_1.$$

Como $H_2 \lhd G$, se tiene $x \star H_2 \star x' \subset H_2$. Luego

$$(x \star y \star x') \star H_1 \in H_2/H_1,$$

de donde $H_2/H_1 \lhd G/H_1$.

2. Basta considerar el epimorfismo proyección $\pi\colon G \longrightarrow G/H_1$ para concluir que $(G/H_1)/(H_2/H_1)$ y G/H_2 son isomorfos.

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Tercer teorema de isomorfía.– Sean G un grupo y N y H subgrupos de G. Supongamos que $N \lhd G$. Entonces:

1. $(N \cap H) \lhd H$ y $N \lhd (NH)$.
2. La inclusión de H en NH induce un isomorfismo de $H/(N \cap H)$ en $(NH)/N$.

Demostración.– Se deja como ejercicio probar $(N \cap H) \lhd H$ y $N \lhd (NH)$. La composición de la inclusión de H en NH con la proyección de NH sobre $(NH)/N$ es un epimorfismo cuyo núcleo coincide con $N \cap H$, de donde el resultado es una consecuencia directa del primer teorema de isomorfía. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Tema 5. Anillos y cuerpos.

5.1. Anillos (I): Unidades y divisores de cero.

Definición.– Un *anillo* es una terna $(A, +, \cdot)$ formada por un conjunto A y dos operaciones internas y binarias $+, \cdot$ verificando:

1. El par $(A, +)$ es un grupo abeliano, cuyo elemento neutro llamaremos normalmente "cero (0)".
2. La operación binaria $\cdot$ es asociativa y tiene elemento neutro, que llamaremos normalmente "uno (1)".
3. La operación $\cdot$ es *distributiva* a la derecha y a la izquierda respecto de la operación $+$, i.e. para todos $x, y, z \in A$, se tiene $(x+y)\cdot z = x\cdot z+y\cdot z$, $x\cdot(y+z) = x\cdot y+x\cdot z$.

Si además la operación $\cdot$ es conmutativa, diremos que el anillo es conmutativo.

Observación.– Algunas notas a la definición.

1. En general se usará la expresión "sea A un anillo", sobreentendiendo las operaciones. La operación $\cdot$ se notará normalmente por simple yuxtaposición.
2. En un anillo A se tiene $0 \cdot x = x \cdot 0 = 0$ para todo $x \in A$.
3. Si en un anillo A se tiene $1 = 0$, entonces $A = \{0\}$.
4. Para todo $x, y \in A$, ese tiene $x(-y) = (-x)y = -(xy)$.
5. Si $A_1, \ldots, A_n$ son anillos, el producto cartesiano $A_1 \times \cdots \times A_n$ posee una estructura natural de anillo, donde las operaciones están definidas componente a componente.

Ejemplos.- Anillos bien conocidos.

1. $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ son anillos conmutativos. La estructura de anillo de $\mathbf{Z}$ viene determinada por la de grupo aditivo: el producto de dos enteros xy coincide con el múltiplo de y con coeficiente x. Así pues, la estructura de anillo de $\mathbf{Z}$ no añade nada nuevo a la de grupo. Esto es falso para $\mathbf{Q}$, $\mathbf{R}$ y $\mathbf{C}$ en los que, obviamente, la estructura multiplicativa no viene determinada por la aditiva.
2. Las congruencias módulo m, $\mathbf{Z}/\mathbf{Z}m$ son un anillo conmutativo con la suma y el producto que hemos definido en el tema 2.
3. El conjunto $\mathcal{M}(n)$ de las matrices $n \times n$ sobre $\mathbf{Z}$, $\mathbf{Z}/\mathbf{Z}p$, $\mathbf{Q}$, $\mathbf{R}$ o $\mathbf{C}$ es un anillo, con respecto a la adición y la multiplicación ordinaria de matrices. No es conmutativo.

4. Si A es un anillo conmutativo, el conjunto $A[x_1, \ldots, x_n]$ de los polinomios en n indeterminadas con coeficientes en A es también un anillo conmutativo.

Definición.– Sea A un anillo. Una *unidad* es un elemento que posee un simétrico multiplicativo (a la izquierda y a la derecha), que llamaremos *inverso*. El conjunto de las unidades de A es un grupo para el producto y se notará A^*.

Un *cuerpo* es un anillo conmutativo tal que todo elemento distinto de cero es una unidad, i.e. $A^* = A - \{0\}$.

Ejemplos.– Algunos casos sencillos de unidades.

1. Las unidades de $\mathbf{Z}$ son $1, -1$.
2. Las unidades de $\mathbf{Z}/\mathbf{Z}n$ son los elementos $a + \mathbf{Z}n$ tales que $\text{mcd}(a, n) = 1$.
3. Los anillos $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ son cuerpos. El anillo $\mathbf{Z}/\mathbf{Z}n$ lo es si y sólo si n es primo.
4. El grupo de las unidades del anillo $\mathcal{M}(n, k)$ con $k = \mathbf{Q}$, $\mathbf{R}$ ó $\mathbf{C}$ es $\text{GL}(n, k)$.

Observación.– A partir de ahora sólo trabajaremos con anillos conmutativos. Así pues, la palabra '*anillo*' significará siempre anillo conmutativo.

Definición.– Sea A un anillo. Un elemento $x \in A$ se llamará un *divisor de cero* si y sólo si es distinto de cero y existe $y \in A$, $y \neq 0$, tal que $xy = 0$. Un anillo sin divisores de cero se llama un *dominio de integridad*.

Un elemento $x \in A$ se llamará *nilpotente* si es distinto de cero y existe un entero $n > 0$ tal que $x^n = 0$.

Observación.– En un dominio de integridad se da la propiedad cancelativa por el producto de elementos no nulos:

$$a \neq 0, ab = ac \Rightarrow b = c.$$

lo cual hace que estos anillos sean particularmente cómodos a la hora de hacer cálculos.

Ejemplos.– Divisores de cero y elementos nilpotentes.

1. Las unidades no son divisores de cero, ya que si x es ambas cosas existirían $y, z \in A$, con $z \neq 0$ tales que $yx = 1$ y $xz = 0$, de donde

   $$z = 1 \cdot z = yxz = y \cdot 0 = 0.$$

   Así, todo cuerpo es un dominio de integridad.

2. $\mathbf{Z}$ es un dominio de integridad.
3. El anillo $\mathbf{Z}/\mathbf{Z}4$ no es un dominio de integridad. El elemento 2 es nilpotente en $\mathbf{Z}/\mathbf{Z}4$.
4. Todos los elementos no nulos de $\mathbf{Z}/\mathbf{Z}n$ son unidades o divisores de cero, pero esto no es cierto en todos los anillos (no lo es, por ejemplo, en $\mathbf{Z}$ o en $k[x]$).

5.2. Anillos (II): Ideales.

El concepto equivalente a subgrupo para anillos no es, como podría esperarse, el de subanillo. En efecto, si $R \subset A$ son dos anillos (con las mismas operaciones) no se puede definir, en general, una estructura coherente de anillo en el grupo cociente A/R.

A mediados del siglo XIX, Dedekind buscaba una generalización de la factorización única en primos que se tiene en $\mathbf{Z}$ para unos anillos denominados *anillos de enteros algebraicos*. Estos anillos, que contienen a $\mathbf{Q}$ y están contenidos en $\mathbf{C}$, no verifican en general que exista una factorización única en elementos irreducibles. Por ello, Dedekind pensó sustituir la factorización tradicional, en producto de elementos del anillo, por un concepto que denomin*élementos ideales*. Conviene destacar que la idea original ya la tuvo Kummer algunos años antes, buscando la demostración del Teorema de Fermat.

Sin embargo, para mantener las propiedades de la divisibilidad tradicional, Dedekind pensó que sus elementos ideales debían verificar las propiedades análogas a la divisibilidad. Esto es:

1. Si $a|b$ y $a|c$, entonces $a|(b+c)$.
2. Si $a|b$, entonces $a|bc$, para todo c.

El resultado de esta magnífica idea fue el concepto que hoy denominamos *ideal de un anillo*.

Definición.– Sea A un anillo. Un *ideal* de A es un subconjunto I de A que verifica:

1. I es un subgrupo del grupo aditivo de A.
2. Para todo $a \in I$, $x \in A$ se tiene $xa \in I$.

Observación.– Sea $I \subset A$ un ideal de A. Se tiene:

1. Si I contiene una unidad, entonces $I = A$.
2. A es un cuerpo si y sólo si sus únicos ideales son $\{0\}$ y A.
3. Los ideales de $\mathbf{Z}$ y los subgrupos son la misma cosa, pues la estructura multiplicativa viene determinada por la aditiva. El apartado anterior prueba entonces de nuevo que $\mathbf{Z}/\mathbf{Z}n$ es un anillo.

Observación.– En realidad no hace falta comprobar que I es un subgrupo aditivo. Para ver si I es ideal es suficiente probar (comparar con las propiedades que buscaba Dedekind):

1. Si $a, b \in I$, entonces $a + b \in I$.
2. Si $a \in I$ y $c \in A$, entonces $ac \in I$.

Asombrosamente, el concepto de Dedekind es precisamente el que permite dotar de estructura de anillo a los cocientes.

Proposición.– El grupo cociente A/I admite una estructura canónica de anillo.

Demostración.– En efecto, basta ver que la fórmula

$$(a+I)(b+I) = ab+I$$

define una operación en A/I.

Si $a+I = a'+I$ y $b+I = b'+I$ es $a-a' \in I$, y $b-b' \in I$. Así

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b-b') + (a-a')b' \in I,$$

lo que prueba nuestro aserto. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.- Sean A, B anillos, $f : A \to B$ una aplicación. Se dirá que f es un *homomorfismo* de anillos si verifica:

1. Para cualesquiera $x, y \in A$, es $f(x+y) = f(x) + f(y)$.
2. Para cualesquiera $x, y \in A$, es $f(xy) = f(x)f(y)$.
3. $f(1) = 1$.

Un homomorfismo biyectivo se llama un *isomorfismo* y los anillos entre los cuales se puede establecer un isomorfismo se llaman anillos isomorfos.

Proposición.– Sea $f : A \longrightarrow B$ un homomorfismo de anillos. Se tienen las siguientes propiedades:

1. El conjunto
$$\ker(f) = \{a \in A \mid f(a) = 0\}$$
es un ideal de A, y f es inyectivo si y sólo si $\ker(f) = \{0\}$.
2. Si $u \in A$ es una unidad, entonces $f(u)$ es una unidad en B. En particular cualquier homomorfismo (de anillos) entre cuerpos es inyectivo.
3. El conjunto
$$\mathrm{im}(f) = \{b \in B \mid \exists a \in A, f(a) = b\}$$
es un subanillo de B (esto es, un anillo dentro de B, con las mismas operaciones).

Primer teorema de isomorfía.– Sea $f : A \longrightarrow B$ un morfismo de anillos. Entonces $A/\ker(f)$ es isomorfo a $\mathrm{im}(f)$.

Segundo teorema de isomorfía.– Sea A un anillo, $I \subset A$ un ideal, y $B \subset A$ un subanillo. Entonces $B + I = \{b + a : b \in B, a \in I\}$ es un subanillo de A, I es un ideal de $B + I$, $B \cap I$ es un ideal de B, y existe un isomorfismo de anillos

$$(B+I)/I \cong B/(B \cap I).$$

Tercer teorema de isomorfía.– Sea A un anillo y sean I, J ideales de A con $I \subset J$. Entonces J/I es un ideal de A/I y A/J es isomorfo a $(A/I)/(J/I)$.

Demostración.– Las tres demostraciones son análogas a las hechas en el tema anterior para homomorfismos de grupos. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$.

Hay que tener cuidado, porque no todas las propiedades de los homomorfismos de grupos se amplían directamente a los homomorfismo de anillos.

Proposición.– Sea $f :\longrightarrow B$ un homomorfismo de anillos.

1. Si $I \subset A$ es un ideal, $f(I)$ *no* es, en general, un ideal de B.
2. Si $I \subset A$ es un ideal y f es sobreyectiva, $f(I)$ es un ideal de B.
3. Si $J \subset B$ es un ideal, $f^{-1}(J)$ es un ideal de A.

Demostración.– Un contraejemplo sencillo para el primer apartado lo da la inclusión $i : \mathbf{Z} \longrightarrow \mathbf{Q}$, dado que $i(\mathbf{Z})$ no es un ideal en $\mathbf{Q}$ (al ser cuerpo, sólo $\{0\}$ y $\mathbf{Q}$ lo son).

En cuando al caso en que f sea sobreyectiva, tomemos $b_1, b_2 \in f(I)$. Entonces tenemos $a_1, a_2 \in I$ tales que $f(a_i) = b_i$ para $i = 1, 2$ y, en ese caso

$$b_1 + b_2 = f(a_1) + f(a_2) = f(a_1 + a_2) \in f(I).$$

Notemos que no hemos usado la sobreyectividad de f aún. Ahora, si tomamos un $y \in B$ *cualquiera*, tenemos que debe existir $x \in A$ con $f(x) = y$ y entonces

$$yb_1 = f(x)f(a_1) = f(xa_1) \in f(I).$$

Para demostrar la tercera propiedad, tomemos $a_1, a_2 \in f^{-1}(I)$. Entonces $f(a_i) \in I$, para $i = 1, 2$, y

$$f(a_1 + a_2) = f(a_1) + f(a_2) \in I,$$

luego $a_1 + a_2 \in f^{-1}(I)$. Por otra parte, si $x \in A$ tenemos que

$$f(xa_1) = f(x)f(a_1) \in I,$$

de donde $xa_1 \in f^{-1}(I)$ y hemos terminado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

5.3. Cuerpo de fracciones. Característica.

Terminamos el desarrollo teórico con dos conceptos importantes: el cuerpo de fracciones, que permite construir un cuerpo a partir de un dominio de integridad, y la característica, que es un elemento crucial a la hora de clasificar cuerpos.

Observación.– Sea A un dominio de integridad y llamemos $A^* = A \setminus \{0\}$. Consideremos la relación binaria $\sim$ definida en $A \times A^*$ por

$$(a, b) \sim (a', b') \;\Leftrightarrow\; ab' = a'b.$$

Es fácil verificar que $\sim$ es una relación de equivalencia. Llamamos $Q(A)$ al conjunto cociente $(A \times A')/\sim$, y los elementos de $Q(A)$ los notaremos como $\frac{a}{b}$, representando así la clase de equivalencia de (a, b).

Se tienen las siguientes operaciones definidas en $Q(A)$:

$$\text{Suma: } \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}.$$

$$\text{Producto: } \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

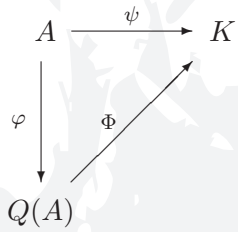
Proposición.– Las operaciones están bien definidas, esto es, si $ab'=a'b$ y $cd'=c'd$, entonces

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

Proposición.– $Q(A)$ es un cuerpo, denominado cuerpo de cocientes o fracciones de A.

Proposición.– Sea A un dominio de integridad y $Q(A)$ su cuerpo de fracciones. Se verifica:

1. La aplicación $\varphi : A \to Q(A)$ definida por $\varphi(a)=\frac{a}{1}$ es un homomorfismo inyectivo de anillos.
2. (*Propiedad universal de* $Q(A)$) Si K es un cuerpo cualquiera, todo homomorfismo inyectivo de anillos $\psi : A \to K$ factoriza por φ, es decir, existe un único homomorfismo de anillos $\Phi : Q(A) \to K$ que hace conmutativo el siguiente diagrama:



3. Si L es un cuerpo que verifica la propiedad anterior de $Q(A)$, entonces L es isomorfo a $Q(A)$.

Se tiene, por tanto, que $Q(A)$ es el menor cuerpo que contiene a un dominio de integridad isomorfo a A, salvo isomorfismo. Dicho de otro modo, todo cuerpo que contiene a un dominio isomorfo a A, contiene también a un cuerpo isomorfo a $Q(A)$.

Demostración.– El primer apartado es trivial. Para el segundo, definimos Φ mediante la expresión

$$\Phi\left(\frac{a}{b}\right)=\psi(a)\psi(b)^{-1}.$$

Hay que verificar que Φ está bien definida:

$$\frac{a}{b}=\frac{a'}{b'} \implies ab'=a'b \implies \psi(a)\psi(b')=\psi(a')\psi(b) \implies \psi(a)\psi(b)^{-1}=\psi(a')\psi(b')^{-1}$$

lo cual prueba que lo está. También tenemos que ver que es un homomorfismo de anillos:

$$\Phi\left(\frac{a}{b}+\frac{a'}{b'}\right)=\Phi\left(\frac{ab'+a'b}{bb'}\right)=\psi(ab'+a'b)\psi(bb')^{-1}=$$

$$= \psi(a)\psi(b)^{-1} + \psi(a')\psi(b')^{-1} = \Phi\left(\frac{a}{b}\right) + \Phi\left(\frac{a'}{b'}\right),$$

y análogamente conserva el producto y el elemento unidad. Se comprueba fácilmente que Φ hace conmutativo el diagrama, y de hecho es la única definición posible para que esto se cumpla, puesto que:

$$\Phi\left(\frac{a}{b}\right) = \Phi\left(\frac{a}{1}\cdot\frac{1}{b}\right) = \Phi\left(\frac{a}{1}\right)\cdot\Phi\left(\frac{1}{b}\right) = \Phi\varphi(a)\Phi\varphi(b)^{-1} = \psi(a)\psi(b)^{-1}.$$

Veamos por último la unicidad del cuerpo de fracciones. Sea L un cuerpo verificando la propiedad universal, con $\varphi' : A \to L$. Tomando $K = Q(A)$, existe $\phi' : L \to Q(A)$ tal que $\varphi = \phi'\varphi'$.

Aplicando 2) a $K = L$ y φ', se tiene que $\varphi' = \Phi\varphi$. De ambas, se tiene $\varphi = \Phi'\Phi\varphi$. Pero aplicando 2) a $K = Q(A)$ y φ, se tiene que $\Phi'\Phi$ y la identidad hacen conmutativo el correspondiente diagrama; por la unicidad se tiene que

$$\Phi'\Phi = \mathrm{id}.$$

Análogamente se tiene que $\Phi\Phi' = \mathrm{id}$, luego Φ es el isomorfismo buscado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Sea K un cuerpo. Todo homomorfismo de anillos φ de $\mathbf{Z}$ en K, lleva el elemento unidad de $\mathbf{Z}$ en el elemento unidad de K. Esto define unívocamente a φ. Por tanto existe un único homomorfismo de anillos φ de $\mathbf{Z}$ en K.

Si el homomorfismo φ de $\mathbf{Z}$ en K es inyectivo, se tiene que K contiene a su cuerpo de fracciones $\mathbf{Q}$. En ese caso diremos que K es un cuerpo de *característica cero*.

Los cuerpos $\mathbf{Q}$, $\mathbf{R}$ y $\mathbf{C}$ son de característica cero, puesto que contienen a $\mathbf{Z}$. Además todo subcuerpo K de $\mathbf{C}$ es de característica cero. En otro caso el homomorfismo $\varphi : \mathbf{Z} \to K$ no inyectivo se extiende a $\mathbf{C}$, contradicción. Por tanto, todo subcuerpo de $\mathbf{C}$ contiene a $\mathbf{Q}$.

Si φ por el contrario no es inyectivo, $\ker(\varphi)$ es un ideal $\mathbf{Z}p$, con $p > 0$. Por el primer teorema de isomorfía $\mathbf{Z}/\mathbf{Z}p$ es isomorfo a un subanillo de K, luego no tiene divisores de cero. Así $\mathbf{Z}/\mathbf{Z}p$ es un dominio de integridad, o equivalentemente un cuerpo, y además, p es un número primo. Diremos entonces que K es un cuerpo de *característica* p. En ese caso se verifica que $px = 0$, para cada $x \in K$.

El ejemplo más simple de cuerpo de característica p es, obviamente, el propio $\mathbf{Z}/\mathbf{Z}p$. De hecho, dar otro ejemplo no trivial es complejo y corresponde a los objetivos de la asignatura *Estructuras Algebraicas*.

5.4. Epílogo: El problema de la factorización.

Finalizamos el contenido teórico de este curso presentando un problema ya mencionado, que esperamos que sirva como motivación para el alumno, al que le presentaremos un problema completamente natural pero que necesitará de más desarrollo teórico para abordar. Es el problema de la factorización en elementos irreducibles.

Definición.– Sea A un anillo. Diremos que $x \in A$ es un elemento irreducible cuando no es una unidad y, si $x = ab$, se tiene forzosamente que a o b son necesariamente unidades.

Observación.– Los elementos irreducibles en $\mathbf{Z}$ son, obviamente, los números primos, mientras que los elementos irreducibles de $k[x]$ son, precisamente, los polinomios irreducibles (de ahí su nombre).

Ejemplo.– Consideremos el elemento $\sqrt{-5} \in \mathbf{C}$. Vamos a formar un anillo con su ayuda, concretamente

$$R = \mathbf{Z}[\sqrt{-5}] = \left\{ a + b\sqrt{-5} \mid a, b \in \mathbf{Z} \right\}.$$

Es muy sencillo comprobar que, con la suma y el producto naturales (heredados de $\mathbf{C}$, por ejemplo), R es un anillo. Así mismo, podemos quedarnos con el concepto de norma, proveniente del módulo de un número complejo:

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

o, escrito en notación compleja, $N(x) = x\,\overline{x}$.

Observación.– No es complicado de ver que la norma verifica las siguientes propiedades:

1. $N : R \longrightarrow \mathbf{N}$.
2. N es una aplicación multiplicativa, esto es $N(xy) = N(x)N(y)$.

La norma puede ayudarnos a entender cómo son los elementos de un anillo de este tipo.

Proposición.– Se verifican las siguientes propiedades:

1. $x \in R$ es una unidad si y sólo si $N(X) = \pm 1$.
2. x e y son asociados si y sólo $x|y$ y $N(x) = N(y)$.
3. Si $N(x)$ es primo, entonces.x es irreducible.

Demostración.– Si $x \in R$ es unidad, entonces existe $y \in R$ tal que $xy = 1$, de donde

$$N(xy) = N(x)N(y) = N(1) = 1,$$

y por tanto, $N(x) = \pm 1$. Al revés, si $N(x) = \pm 1$ construimos explícitamente un inverso de $x = a + b\sqrt{-5}$,

$$x^{-1} = \frac{\overline{x}}{N(x)} \in R.$$

La segunda afirmación se sigue directamente de la primera (y de la definición de elementos asociados).

Ahora, si $N(x)$ es primo y $x = ab$, entonces $N(x) = N(a)N(b)$, por lo que bien $N(a)$, bien $N(b)$, por ser enteros, han de ser ± 1 y por tanto, bien a, bien b son unidad. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Fijémonos entonces en cómo podríamos factorizar elementos en R. Obviamente, la demostración de que existe una factorización en producto de irreducibles sigue siendo

válida. En efecto, partimos de x y, si es irreducible, hemos terminado y si no es producto de dos elementos de norma estrictamente menor, lo que nos permite aplicar la inducción.

Sin embargo, lo que no está tan claro es que la factorización en irreducibles sea única. Por ejemplo, podemos escribir

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

Claramente no son *la misma* factorización porque

$$N(2) = 4, \qquad N(3) = 9, \qquad N\left(1 \pm \sqrt{-5}\right) = 6,$$

de forma que los factores que hemos encontrado no son asociados. Aún así, bien podría haber alguna factorización más detallada, o sea, algún irreducible p que dividiese, por ejemplo, a 2 y a $1 + \sqrt{-5}$. Pero p no puede ser entero, porque 2 es primo, y no puede tener parte compleja, porque entonces $N(p) \geq 5$ luego no puede dividir a 2.

Por tanto, independientemente de si 2, 3 y $1 \pm \sqrt{-5}$ son o no irreducibles, las descomposiciones anteriores nos llevarán a dos factorizaciones distintas.

Definición.– Un anillo A, sin divisores de cero, en el cual todo elemento se puede descomponer de manera única (salvo unidadaes) como producto de irreducibles se denomina un *dominio de factorización única* (abreviadamente DFU).

En general el problema de determinar si un anillo posee o no factorización única no es sencillo, aunque sabemos algunos ejemplos muy especiales.

Proposición.– Sea A un anillo en el que todo ideal puede ser generado por un sólo elemento (estos anillos se llaman *dominios de ideales principales* o DIP). Entonces A es un DFU.

Demostración.– La demostración no es complicada, pero sí un poco larga. Los pasos son los siguientes:

1. Primero demostramos que, si A es un DIP, entonces toda cadena de ideales creciente

   $$I_1 \subset I_2 \subset ... \subset I_n \subset ...$$

   es estacionaria, esto es, existe un $r \in \mathbf{N}$ tal que $I_r = I_s$ para todo $s > n$.

2. Utilizando esto, demostramos que todo elemento se descompone en factores irreducibles de manera finita.

3. Dados dos elementos $x, y \in A$, como existe d tal que $\langle x, y\rangle = \langle d\rangle$, probamos que un tal d es *un* máximo común divisor de x e y. Y probamos el Teorema de Euclides: si p es un irreducible tal que $p|xy$ pero mcd$(p, x) = 1$, entonces $p|y$.

4. Finalmente, probamos que el Teorema de Euclides es equivalente a la unicidad de la factorización. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Sea A un dominio tal que existe una función $\mu : A \longrightarrow \mathbf{N} \cup \{0\}$ verificando:

1. Para cualesquiera $x \in A$, $y \in A \setminus \{0\}$, existe unos únicos $q, r \in A$ tales que

   $$a = qb + r, \text{ con } \mu(r) < \mu(b).$$

2. $\mu(a) = 0 \iff a = 0$.

A este procedimiento se le llama *división euclídea* de A y, en estas condiciones, A se denomina un *dominio euclídeo* (abreviadamente DE).

Observación.– Z y $k[x]$ son DE, como hemos visto durante el curso, tomando respectivamente, $\mu = |\cdot|$ y $\mu =$grado$+1$. Pero muy pocos anillos lo son, en realidad. Por ejemplo $k[x, y]$ no lo es, como veremos ahora.

Proposición.– Un DE es un DIP (y, por tanto, un DFU).

Demostración.– La demostración consiste en, dado un ideal I, tomar $d \in I$ tal que

$$\mu(d) = \min_{x \in I} \{\mu(x) \mid x \in I\},$$

y probar (no es complicado) que $I = \langle d \rangle$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Ejemplo.– El anillo $k[x, y]$ no es un DE porque no es un DIP, como se puede ver considerando $\langle x, y \rangle$.

En la construcción de DFU, curiosamente, los DE juegan un papel destacado, gracias al resultado siguiente, con el que terminamos esta sección.

Teorema.– Sea A un DFU. Entonces $A[x]$ también es un DFU.

Demostración.– Comenzamos por definir, como hicimos en el tema 4, el contenido de un polinomio como el mcd de sus coeficientes. A partir de aquí definimos el concepto de polinomio primitivo (exactamente igual) y probamos que

$$c(fg) = c(f)c(g),$$

así como el Lema de Gauss (el producto de polinomios primitivos es primitivo). Con esto, dado un polinomio primitivo $f(x) \in A[x]$ lo factorizamos en $Q(A)[x]$ en producto de irreducibles, cosa que podemos hacer porque $Q(A)[x]$ es un DE y por tanto un DFU:

$$f(x) = p_1(x)...p_r(x),$$

y extraemos un mcm de los denominadores que aparecen en los factores, para escribir

$$f(x) = \frac{1}{m} q_1(x)...q_r(x),$$

con $m \in A$ y $q_1(x), ..., q_r(x)$ irreducibles en $A[x]$. Ahora bien, por ser $f(x)$ primitivo se tiene que ha de ser $m = 1$, luego $p_i(x) = q_i(x)$ para cada $i = 1, ..., r$.

Con esto aseguramos la factorización, mientras que la unicidad viene dada porque dos factorizaciones distintas en $A[x]$ inducen dos factorizaciones distintas en $Q(A)[x]$, lo cual es imposible por ser $Q(A)[x]$ un DFU. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Continuará...