# Álgebra básica

Manuel Bullejos Lorenzo
Pilar Carrasco Carrasco
Pedro García Sánchez
Antonio Martínez Cegarra
Eugenio Miranda Palacios
Antonio Rodríguez Garzón

Curso 2008-2009

# Índice general

# Capítulo 1

# Aritmética entera

## 1.1. El anillo ordenado de los números enteros

Los números enteros son familiares en la aritmética elemental. Aquí queremos expresar esta familiaridad en términos precisos. Enunciaremos una lista de propiedades que poseen los enteros y a partir de ellas sacaremos nuestras deducciones. Todas estas propiedades pueden deducirse de una lista muy corta de axiomas, pero de momento esto es inmaterial.

Denotamos $\mathbb{N}$ al conjunto de los enteros positivos (también llamados números naturales) $\{1, 2, 3, \dots\}$. y denotamos por $\mathbb{Z}$ al conjunto de todos los enteros positivos, negativos y nulo. La letra $\mathbb{N}$ es la inicial de la palabra *número* y $\mathbb{Z}$ es la inicial de *Zahl* (número en alemán). En matemáticas está muy extendido el uso de ambas abreviaturas.

En el conjunto $\mathbb{Z}$ hay definidas tres operaciones: Suma, $x+y$, resta o sustracción , $x-y$ y multiplicación $x \cdot y$ o $xy$. Con frecuencia es conveniente expresar la resta sumando el opuesto, $x - y = x + (-y)$. Estas operaciones verifican las siguientes propiedades:

**Ley asociativa** $(x + y) + z = x + (y + z), \qquad (xy)z = x(yz)$

**Ley conmutativa** $x + y = y + x \qquad xy = yx$

**Existencia de neutro** $x + 0 = x \qquad x1 = x$

**Existencia de opuesto** $x + (-x) = 0.$

El número 0 se llama *neutro para la suma* porque al sumarlo a cualquier número $x$ el resultado es igual a $x$. De la misma forma el número 1 es *neutro para la multiplicación*. Todo entero $x$ tiene el opuesto $-x$, pero salvo 1 y $-1$ ningún entero tiene un inverso multiplicativo. Mas adelante hallaremos inversos para todo entero no nulo cuando veamos los números racionales.

Además de las propiedades anteriores, existe otra propiedad que relaciona la suma y el producto:

**Ley distributiva** $x(y + z) = xy + xz.$

Un conjunto $R$ con dos operaciones $x + y$, $xy$ verificando las anteriores propiedades se llama *anillo conmutativo*, así que el conjunto $\mathbb{Z}$ de todos los enteros es un anillo conmutativo. Sin embargo estas leyes no son suficientes para determinar unívocamente a $\mathbb{Z}$.

Veamos ahora algunas consecuencias de las leyes anteriores: De la ley distributiva se sigue que para todo $x \in \mathbb{Z}$ se verifica $x \cdot 0 = 0 = 0 \cdot x$. Por la ley asociativa, la suma de cualquier número de términos es independiente de la manera en que introduzcamos paréntesis, y por la ley conmutativa el orden de

los términos no altera la suma. Igual ocurre con la multiplicación. De momento aceptamos todo esto sin demostraciones.

La suma de los números $a_1, \ldots, a_n$ se puede escribir $a_1 + \cdots + a_n$. Normalmente se abrevia esta expresión escribiendo el término general $a_i$ precedido de una sigma mayúscula $\Sigma$ con alguna indicación del rango en que se suman los enteros (excepto si esto último está claro del contexto). Así que en lugar de $a_1 + \cdots + a_n$ podemos escribir

$$\Sigma_{i=1}^{n} a_i, \qquad \Sigma_1^n a_i, \qquad \Sigma_i a_i, \qquad \Sigma a_i$$

donde en cada caso $i$ es una *variable muda*. Cuando $n = 0$ la suma escrita es vacía y, por convención, se toma igual a cero.

Existe una abreviatura similar para productos repetidos usando la pi mayúscula en lugar de $\Sigma$. Así que en lugar de $a_1 a_2 \ldots a_n$ podemos escribir

$$\Pi_{i=1}^{n} a_i, \qquad \Pi_1^n a_i, \qquad \Pi_i a_i, \qquad \Pi a_i$$

Por ejemplo, podemos definir la función factorial como $n! = \Pi_1^n i$. Un producto vacío se toma igual a uno; así que las sumas vacías y los productos vacíos son respectivamente neutros para la suma y el producto.

Una propiedad importante de los enteros es que el producto de dos enteros no nulos no es nunca cero:

**Ley de integridad** Para cualesquiera enteros $a, b$, si $a \neq 0$ y $b \neq 0$ entonces $ab \neq 0$. Además $1 \neq 0$

Esto tiene una consecuencia muy útil:

**Ley cancelativa** Para cualesquiera $a, b, c \in \mathbb{Z}$ si $ca = cb$ y $c \neq 0$ entonces $a = b$.

Esto asegura que "multiplicación por un entero no nulo" es una aplicación inyectiva de $\mathbb{Z}$ en sí mismo. Para demostrarlo, supongamos que $a \neq b$, entonces $a - b \neq 0$ y por la ley de integridad $c(a - b) \neq 0$, por tanto $ca - cb = c(a - b) \neq 0$.

En $\mathbb{Z}$ además de las operaciones existe una relación de orden que escribimos $x \leq y$ o $y \geq x$. Si $x \leq y$ pero $x \neq y$ escribimos $x < y$ y también $y > x$. Esta relación es una *relación de orden total* y está relacionada con las operaciones de $\mathbb{Z}$ por las siguientes reglas:

Si $x_1 \leq x_2$, $y_1 \leq y_2$ entonces $x_1 + y_1 \leq x_2 + y_2$.

Si $x \leq y$ y $z > 0$ entonces $zx \leq zy$.

Estas reglas indican que $\mathbb{Z}$ es un *anillo totalmente ordenado*. Usando la ordenación podemos describir el conjunto $\mathbb{N}$ de los enteros positivos como:

$$\mathbb{N} = \{x \in \mathbb{Z} \mid x > 0\} \tag{1.1.1}$$

Es costumbre tomar $\mathbb{N}$ como conjunto de partida dado por algunos axiomas (normalmente los *axiomas de Peano*) y a partir de él se construye $\mathbb{Z}$.

Nótese que para todo $x \in \mathbb{Z}$ se verifica que $x = 0$ o $x \in \mathbb{N}$ o $-x \in \mathbb{N}$ y que estas tres posibilidades son mutuamente excluyentes. De hecho esto es cierto en cualquier anillo ordenado, definiendo $\mathbb{N}$ por la regla 1.1.1, debido a que el orden es total.

## 1.2. Inducción. Principios del mínimo y del máximo

Para fijar $\mathbb{Z}$ completamente utilizamos la siguiente condición sobre el conjunto $\mathbb{N}$ de los enteros positivos:

**I. Principio de inducción** sea $S$ un subconjunto de $\mathbb{N}$ tal que $1 \in S$ y que $n \in S \Rightarrow n+1 \in S$. Entonces $S = \mathbb{N}$.

Este principio forma la base del método familiar de *demostración por inducción*: Sea $P(n)$ una afirmación acerca de un entero positivo $n$ (p. e., $P(n)$ = "la suma de los $n$ primeros enteros positivos es $n(n+1)/2$") Supongamos que queremos demostrar $P(n)$ para todo $n$. Para ello por el principio de inducción basta demostrar $P(1)$ y demostrar $\forall n(P(n) \Rightarrow P(n+1))$, porque esto significa que el conjunto $S = \{n \in \mathbb{N} \mid P(n)\}$ contiene a 1 y que si contiene a $n$ también contiene a $n+1$. Del principio de inducción se deduce que $S = \mathbb{N}$, es decir que todo $n \in \mathbb{N}$ verifica $P(n)$.

Existen formas alternativas del principio de inducción que se usan con frecuencia:

**II. Principio de inducción alternativo** Sea $S$ un subconjunto de $\mathbb{N}$ tal que $1 \in S$ y que $n \in S$ siempre que para todo $m < n$ $m \in S$. Entonces $S = \mathbb{N}$.

**III. Principio del mínimo o principio de buena ordenación.** Todo conjunto no vacío de enteros positivos tiene un elemento mínimo.

**IV. Principio del máximo** Todo conjunto no vacío de enteros negativos tiene un elemento máximo.

El principio del mínimo se suele enunciar diciendo que $\mathbb{N}$ está *bien ordenado*

Veamos la equivalencia de los principios enunciados:

**I $\Rightarrow$ II** : Sea $S$ un conjunto verificando las hipótesis de **II**. Definimos $T = \{x \in \mathbb{N} \mid \forall y(y \leq x \Rightarrow y \in S)\}$, es decir que $x \in T$ precisamente cuando todos los números desde 1 hasta $x$ pertenecen a $S$. Es evidente que $T \subseteq S$, así que basta demostrar que $T = \mathbb{N}$. Como $1 \in S$, tenemos que $1 \in T$. Si $n \in T$ entonces $y \in S$ para todo $y \leq n$, luego $n+1 \in S$ y por tanto $y \in S$ para todo $y \leq n+1$. Pero esto implica que $n+1 \in T$. Por **I** tenemos que $T = \mathbb{N}$.

**II $\Rightarrow$ III** : Sea $S$ un conjunto de enteros positivos que no tiene elemento mínimo. Vamos a demostrar que $S$ es el conjunto vacío: Llamamos $S' = \{x \in \mathbb{N} \mid x \notin S\}$ al complemento de $S$. Como $S$ no tiene primer elemento, $1 \notin S$ luego $1 \in S'$. Si para todo $m \leq n$ se verifica que $m \in S'$, necesariamente $n \in S'$ (porque en otro caso $n \in S$ y $n$ sería un elemento mínimo para $S$). Por **II**, $S' = \mathbb{N}$ y por tanto $S = \emptyset$.

**III $\Rightarrow$ I** : El elemento mínimo de $\mathbb{N}$ es 1. Sea $S$ un subconjunto de $\mathbb{N}$ que verifique las hipótesis del principio de inducción. Sea $S' = \{x \in \mathbb{N} \mid x \notin S\}$. Sabemos que $1 \notin S'$ y si $n \in S'$ entonces $n-1 \in S'$. Luego $S'$ no tiene elemento mínimo, por tanto es el conjunto vacío y $S = \mathbb{N}$.

**III $\Rightarrow$ IV** : Sea $S$ un conjunto no vacío de enteros negativos. Entonces $T = \{x \in \mathbb{Z} \mid -x \in S\}$ es un conjunto no vacío de elementos positivos. Por **III** $T$ tiene elemento mínimo, sea $n$. Entonces $-n \in S$ y para todo $m \in S$ tenemos que $-m \in T$, luego $n \leq -m$ lo que equivale a $-n \geq m$ para todo $m \in T$, así que $-n$ es el elemento máximo de $S$.

**IV $\Rightarrow$ III** : Se demuestra de manera análoga al apartado anterior.

## 1.3. Divisibilidad

**Definición 1.3.1.** Dados $a, b \in \mathbb{Z}$ decimos que *$b$ divide $a$*, que *$a$ es divisible por $b$* y que *$a$ es un múltiplo de $b$* si existe un $c \in \mathbb{Z}$ tal que $a = bc$. Lo denotamos por $b \mid a$.

Ya que cualquier múltiplo de 0 es 0, se verifica que $0 \mid a$ sólo cuando $a = 0$. Por esta razón en la expresión $b \mid a$ normalmente se toma $b \neq 0$. Para todo $b \in \mathbb{Z}$ se verifica que $b \mid 0$.

La negación de $b \mid a$ se escribe $b \nmid a$ que significa que $a$ no es divisible por $b$. La relación de divisibilidad en $\mathbb{Z}$ satisface las siguientes propiedades:

1. $c \mid b$ y $b \mid a$ implican $c \mid a$. Transitiva
2. Para todo $a \in \mathbb{Z}$ se verifica que $a \mid a$. En sí mismo
3. Si $a \mid b$ y $b \mid a$ entonces $a = \pm b$.

   Estas tres propiedades muestran que la divisibilidad es un orden parcial en el conjunto de enteros positivos.
4. $b \mid a$, $a > 0$ y $b > 0$ implican $b \leq a$
5. $b \mid a_1$ y $b \mid a_2$ implican que $b \mid (xa_1 + ya_2)$ para cualesquiera $x, y \in \mathbb{Z}$. En particular $b \mid (a_1 - a_2)$.
6. $b \mid a$ implica que para todo $c \in \mathbb{Z}$ se verifica $b \mid ac$.
7. Si $c \neq 0$, $b \mid a$ si y sólo si $cb \mid ca$

**Definición 1.3.2.** Dos enteros $a, b$ tales que $b \mid a$ y $a \mid b$ se llaman *asociados*.

De la propiedad 3 anterior vemos que todo entero $a$ está asociado a un único entero no negativo, que se llama su *valor absoluto* y se representa por $|a|$.

## 1.4. Algoritmo de la división euclídea

La primera aplicación del principio de buena ordenación es demostrar el *algoritmo de la división*:

**Teorema 1.4.1.** *Para cualesquiera enteros $a$ y $b$, con $b > 0$, existen enteros únicos $q$ (el cociente) y $r$ (el resto) tales que $a = bq + r$ con $0 \leq r < b$.*

*Demostración.* Consideramos el conjunto $R = \{s = a - bq \mid q \in \mathbb{Z},\ s \geq 0\}$. Como $b > 0$, el elemento $a - b(-|a|) = a + b \cdot |a|$ es mayor o igual a cero y está en $R$. Luego $R$ no es vacío.

Por el principio de buena ordenación $R$ tiene un primer elemento, al que llamamos $r$. Por definición $r = a - bq \geq 0$, y $a = bq + r$. Si fuera $r \geq b$, entonces $s = r - b = a - b(q + 1) \geq 0$, luego $s \in R$ y $s < r$. Esto contradice la minimalidad de $r$, luego $r < b$.

Para demostrar que $q$ y $r$ son únicos, supongamos que $a = bq + r = bp + s$ con $0 \leq r, s < b$. Esto implica que $|r - s| < b$. Pero $r - s = b(q - p)$ lo que muestra que $b \mid (r - s)$. El único múltiplo de $b$ con menor valor absoluto que $b$ es el cero, luego $r - s = 0$ y por tanto $r = s$. Además $bp = bq$, lo que implica $p = q$. □

**Corolario 1.4.2.** *Dados dos enteros $a$ y $b$ con $b > 0$, $b \mid a$ si y sólo si el resto de la división de $a$ por $b$ es 0.*

**Definición 1.4.3.** Para $a \in \mathbb{Z}$ definimos el conjunto de todos los múltiplos de $a$ como $a\mathbb{Z} = \{aq \mid q \in \mathbb{Z}\}$.

**Proposición 1.4.4.** *El conjunto $a\mathbb{Z}$ es cerrado para la suma y la resta.*

**Teorema 1.4.5.** *Sea $I$ un conjunto no vacío de enteros que es cerrado para la suma y la resta. Entonces o $I$ sólo contiene al cero o contiene un mínimo elemento positivo $a$, en cuyo caso $I = a\mathbb{Z}$.*

*Demostración.* Ya que $I$ no es vacío, o sólo contiene al cero o contiene algún entero no nulo $b$. En el primer caso hemos terminado. En el segundo caso, $I$ contiene a $b - b = 0$ y a $0 - b = -b$. Así que $I$ contiene al entero positivo $|b|$. Luego el conjunto $I^+$ de enteros positivos de $I$ no es vacío. Por el principio de buena ordenación tiene un elemento mínimo, al que llamamos $a$.

Cualquier múltiplo de $a$ se obtiene sumando $a$ o $-a$ consigo mismo un número finito de veces, luego $a\mathbb{Z} \subseteq I$.

Por otra parte, sea $c \in I$ arbitrario. Dividimos entre $a$, así que $c = aq + r$ con $0 \leq r < a$. Pero $r = c - aq \in I$. Por el carácter minimal de $a$, debe ser $r = 0$. O sea, que $c = aq \in a\mathbb{Z}$. Como $c$ era un elemento arbitrario de $I$, obtenemos que $I \subseteq a\mathbb{Z}$. Combinando con el párrafo anterior nos queda que $I = a\mathbb{Z}$. □

## 1.5. Máximo común divisor y mínimo común múltiplo

**Definición 1.5.1.** Un entero positivo $d$ se llama *máximo común divisor* de dos enteros dados $a$ y $b$ si

1. $d$ es un divisor de $a$ y $b$
2. Todo divisor común de $a$ y $b$ es un divisor de $d$.

El máximo común divisor de $a$ y $b$ se representa como $d = \text{m. c. d.}(a, b)$ y también como $d = (a, b)$.

El hecho de enunciar una definición del máximo común divisor (o de cualquier otro concepto) no garantiza su existencia. Además debemos justificar el uso del artículo determinado "el", ya que implica su unicidad. Este último punto es fácil de tratar: Si $d_1$ y $d_2$ son máximos comunes divisores de $a$ y $b$, entonces la definición requiere que $d_1 \mid d_2$ y $d_2 \mid d_1$, luego $d_2 = \pm d_1$. Ya que ambos son positivos, $d_2 = d_1$.

**Definición 1.5.2.** Sean $a, b \in \mathbb{Z}$. Cualquier entero de la forma $ma + nb$ con $m, n \in \mathbb{Z}$ se llama *combinación lineal de $a$ y $b$*.

El siguiente teorema muestra la existencia del máximo común divisor de dos enters cualesquiera y su expresión como combinación lineal de ambos:

**Teorema 1.5.3.** *Dos enteros no nulos arbitrarios $a$ y $b$ tienen un máximo común dívisor, que se puede expresar como la menor combinación lineal positiva de $a$ y $b$.*

*Además un entero es una combinación lineal de $a$ y $b$ si y sólo si es un múltiplo de su máximo común divisor.*

*Demostración.* Sea $I$ el conjunto de todas las combinaciones lineales de $a$ y $b$, es decir

$$I = \{x \in \mathbb{Z} \mid x = ma + nb,\ m, n \in \mathbb{Z}\}$$

El conjunto $I$ no es vacío, porque contiene a los elementos $a = 1 \cdot a + 0 \cdot b$ y $b = 0 \cdot a + 1 \cdot b$. Es fácil comprobar que $I$ es cerrado para la suma y la resta. Por el teorema 1.4.5, $I = d\mathbb{Z}$, siendo $d$ el menor entero positivo de $I$.

Como $d \in I$, existen $m, n \in \mathbb{Z}$ tales que $d = ma + nb$. Como $a, b \in I$, necesariamente $d \mid a$ y $d \mid b$.

Sea ahora $c \in \mathbb{Z}$ tal que $c \mid a$ y $c \mid b$, así que $a = cq_1$ y $b = cq_2$. Entonces

$$d = ma + nb = mcq_1 + ncq_2 = c(mq_1 + nq_2)$$

lo que muestra que $c \mid d$.

La última afirmación se sigue del hecho de que $I$ (el conjunto de todas las combinaciones lineales de $a$ y $b$) es igual a $d\mathbb{Z}$ (el conjunto de todos los múltiplos de $d$). □

La igualdad $d = ma + nb$ donde $d = (a, b)$ se conoce como *igualdad de Bezout*.

**Corolario 1.5.4.** *Para cualquier entero positivo $c$, $(ca, cb) = c \cdot (a, b)$.*

*Demostración.* Por el teorema 1.5.3 tenemos que $(ca, cb)$ es el menor valor positivo de $cax + cby$, que es igual al producto de $c$ por el menor valor positivo de $ax + by$, es decir el producto de $c$ por $(a, b)$. □

**Corolario 1.5.5.** *Si $c \mid a$, $c \mid b$ y $c > 0$, entonces*

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b)$$

*Si $(a, b) = d$ entonces $(a/d, b/d) = 1$.*

*Demostración.* La primera afirmación es consecuencia directa del corolario anterior reemplazando $c, a, b$ en dicho corolario por $c, a/c, b/c$ respectivamente. La segunda afirmación es un caso particular de la primera. □

**Definición 1.5.6.** Dos enteros $a, b$ se llaman *primos relativos* si $(a, b) = 1$, es decir si no tienen divisores comunes salvo $\pm 1$.

**Teorema 1.5.7.** *Para cualquier $c \in \mathbb{Z}$, $(a, b) = (b, a) = (a, -b) = (a, b + ac)$.*

**Teorema 1.5.8.** *1. Si $b \mid ac$, entonces $b \mid (a, b)c$.*

2. *Si $b \mid ac$ y $(a, b) = 1$ entonces $b \mid c$.*
3. *Si $b \mid a$, $c \mid a$ y $(b, c) = 1$ entonces $bc \mid a$.*
4. *$(a, bc) = 1$ si y sólo si $(a, b) = 1$ y $(a, c) = 1$.*

*Demostración.* 1. Supongamos que $b \mid ac$. Sea $ac = bq$. Escribimos $(a, b) = ma + nb$ para algunos $m, n \in \mathbb{Z}$. Multiplicando por $c$ obtenemos $(a, b)c = mac + nbc = (mq + nc)b$.

2. Simplemente tomamos $(a, b) = 1$ en el apartado anterior.

3. Sea $a = bq$. Si $c \mid a = bq$ y por el apartado anterior $c \mid q$, sea $q = cq_1$. Sustituyendo obtenemos $a = bcq_1$, luego $bc \mid a$.

4. Sea $(a, bc) = 1$. Entonces $ma + n(bc) = 1$ para algunos $m, n \in \mathbb{Z}$. Podemos escribir esta igualdad de otras dos formas: $ma + (nc)b = 1$, $ma + (nb)c$ que muestran que $(a, b) = 1$ y $(a, c) = 1$.

   A la inversa, existen enteros $m_1, m_2, n_1, n_2$ tales que $1 = m_1a + n_1b = m_2a + n_2c$. Multiplicando y agrupando términos queda: $1 = (m_1m_2a + n_1m_2b + m_1n_2c)a + n_1n_2bc$, luego $(a, bc) = 1$.

□

Probablemente estamos acostumbrados a calcular el máximo común divisor de $a$ y $b$ mediante el cálculo de sus factorizaciones en primos. Esta técnica es efectiva para números pequeños, y la estudiaremos mas adelante. Pero en la práctica, puede ser muy largo hallar los factores primos de números grandes, mientras que el máximo común divisor se encuentra en muchos menos pasos usando el método que vamos a describir a continuación.

El máximo común divisor de dos números puede calcularse utilizando un procedimiento conocido como *algoritmo de Euclides* (nuestra demostración del teorema 1.4.5 no incluye un método explícito para calcularlo). Para describir el algoritmo de Euclides necesitamos las siguientes propiedades:

**Lema 1.5.9.** *1. Si $a \neq 0$ y $b \mid a$, entonces $(a, b) = |b|$*

2. *Si* $a = bq + r$, *entonces* $(a, b) = (b, r)$.

*Demostración.* 1. Todo divisor de $b$ es un divisor de $a$. Y todo divisor de $b$ divide a $|b|$. Aplicando directamente la definición de máximo común divisor obtenemos el resultado buscado.

2. El elemento $a$ es una combinación lineal de $b$ y $r$, luego $(b, r) \mid a$. Ya que también $(b, r) \mid b$ obtenemos que $(b, r) \mid (a, b)$. Como $r = a - bq$ es una combinación lineal de $a$ y $b$, un argumento similar muestra que $(a, b) \mid (b, r)$ y por tanto $(a, b) = (b, r)$.

□

Dados enteros $a > b > 0$ el algoritmo de Euclides utiliza repetidamente el algoritmo de la división para obtener

$$\begin{aligned} a &= bq_1 + r_1 && \text{con} \quad 0 \leq r_1 < b \\ b &= r_1 q_2 + r_2 && \text{con} \quad 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 && \text{con} \quad 0 \leq r_3 < r_2 \\ & && \text{etc.} \end{aligned}$$

Ya que $r_1 > r_2 > \cdots \geq 0$, los restos van menguando y tras un número finito de pasos obtenemos un resto $r_{n+1} = 0$. El algoritmo acaba con la ecuación

$$r_{n-1} = r_n q_{n+1} + 0$$

Esto nos da el máximo común divisor:

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n$$

*Ejemplo* 1.5.10. Para mostrar que $(24, 18) = 6$ tenemos:

$$\begin{aligned} 24 &= 18 \cdot 1 + 6 & (24, 18) &= (18, 6) \\ 18 &= 6 \cdot 3 + 0 & (18, 6) &= 6 \end{aligned}$$

*Ejemplo* 1.5.11. Veamos que $(126, 35) = 7$:

$$\begin{aligned} 126 &= 35 \cdot 3 + 21 & (126, 35) &= (35, 21) \\ 35 &= 21 \cdot 1 + 14 & (35, 21) &= (21, 14) \\ 21 &= 14 \cdot 1 + 7 & (21, 14) &= (14, 7) \\ 14 &= 7 \cdot 2 + 0 & (14, 7) &= 7 \end{aligned}$$

*Ejemplo* 1.5.12. Calculamos $(83, 38) = 1$:

$$\begin{aligned} 83 &= 38 \cdot 2 + 7 & (83, 38) &= (38, 7) \\ 38 &= 7 \cdot 5 + 3 & (38, 7) &= (7, 3) \\ 7 &= 3 \cdot 2 + 1 & (7, 3) &= (3, 1) \\ 3 &= 1 \cdot 3 + 0 & (3, 1) &= 1 \end{aligned}$$

Si sólo se necesita calcular el máximo común divisor, paramos en cuanto podamos calcularlo en la cabeza. Para mostrar que $(83, 38) = 1$, nótese que ya que 7 no tiene divisores positivos salvo 1 y 7 y no es un divisor de 38, es claro de inmediato que $(38, 7) = 1$.

*Ejemplo* 1.5.13. A veces queremos conocer la combinación lineal de $a$ y $b$ que nos da $(a, b)$. Al calcular $(126, 35)$ en el ejemplo 1.5.11 tenemos las siguientes ecuaciones:

$$\begin{aligned} a &= bq_1 + r_1 & 126 &= 35 \cdot 3 + 21 \\ b &= r_1q_2 + r_2 & 35 &= 21 \cdot 1 + 14 \\ r_1 &= r_2q_3 + r_3 & 21 &= 14 \cdot 1 + 7 \\ r_2 &= dq_4 + 0 & 14 &= 7 \cdot 2 + 0 \end{aligned}$$

El siguiente paso es despejar el resto no nulo en cada una de las ecuaciones, omitiendo la última y sustituyendo los anteriores para expresarlos como combinación lineal de $a$ y $b$:

$$\begin{aligned} r_1 &= a + (-q_1)b \\ r_2 &= b + (-q_2)r_1 & &= (-q_2)a + (1 + q_1q_2)b \\ d &= r_1 + (-q_3)r_2 & &= (1 + q_2q_3)a + (-q_1 - q_3 - q_1q_2q_3)b \end{aligned}$$

es decir:

$$\begin{aligned} 21 &= 126 + (-3)35 \\ 14 &= 35 + (-1)21 & &= (-1)126 + 4 \cdot 35 \\ 7 &= 21 + (-1)14 & &= 2 \cdot 126 - 7 \cdot 35 \end{aligned}$$

La técnica usada en el ejemplo precedente puede extenderse fácilmente a la situación general en que se quiere expresar $(a, b)$ como una combinación lineal de $a$ y $b$. Después de despejar para el resto en cada ecuación relevante nos queda

$$\begin{aligned} &\dots \\ r_{j-1} &= r_{j-3} + (-q_{j-1})r_{j-2} & &= m_{j-1}a + n_{j-1}b \\ r_j &= r_{j-2} + (-q_j)r_{j-1} & &= m_ja + n_jb \\ r_{j+1} &= r_{j-1} + (-q_j)r_j & &= m_{j+1}a + n_{j+1}b \\ &\dots \end{aligned}$$

donde $m_{j+1} = m_{j-1} - q_jm_j$ y $n_{j+1} = n_{j-1} - q_jn_j$.

El algoritmo de Euclides puede expresarse en una forma matricial conveniente que arrastra al mismo tiempo los restos y las combinaciones lineales: Empezamos con la matriz

$$\begin{matrix} a & 1 & 0 \\ b & 0 & 1 \end{matrix}$$

y dividimos $a = bq_1 + r_1$. La tercera fila de la matriz se obtiene restando a la primera el producto de la segunda por $q_1$:

$$\begin{matrix} a & 1 & 0 \\ b & 0 & 1 \\ r_1 & 1 & -q_1 \end{matrix}$$

Ahora tomamos $b = r_1q_2 + r_2$ y restamos el producto de $q_2$ por la tercera fila de la segunda:

$$\begin{matrix} a & 1 & 0 \\ b & 0 & 1 \\ r_1 & 1 & -q_1 \\ r_2 & -q_2 & 1 + q_1q_2 \end{matrix}$$

Es fácil comprobar que este algoritmo produce filas sucesivas $(r_j\ m_j\ n_j)$ compuestas de los restos $r_j$ y los coeficientes tales que $r_j = m_j a + n_j b$. Se continúa el proceso hasta que el primer coeficiente de la fila es 0. En ese momento la penúltima fila nos da el máximo común divisor y los coeficientes de la combinación lineal buscada.

*Ejemplo* 1.5.14. Usamos la forma matricial del algoritmo de Euclides para calcular una vez mas el máximo común divisor de $a = 126$ y $b = 35$:

$$\begin{array}{ccc} 126 & 1 & 0 \\ 35 & 0 & 1 \\ 21 & 1 & -3 \\ 14 & -1 & 4 \\ 7 & 2 & -7 \\ 0 & -5 & 18 \end{array}$$

y obtenemos que $(126, 35) = 7 = 2 \cdot 126 - 7 \cdot 35$.

La última línea $0 = -5 \cdot 126 + 18 \cdot 35$ también nos da información interesante: Podemos sumar cualquier múltiplo de esta combinación lineal a la representación anterior del máximo común divisor. Por ejemplo, $7 = (-3) \cdot 126 + 11 \cdot 35$ y también $7 = (-8) \cdot 126 + 29 \cdot 35$.

*Ejemplo* 1.5.15. En forma matricial, el cálculo de $(83, 38)$ es el siguiente:

$$\begin{array}{ccc} 83 & 1 & 0 \\ 38 & 0 & 1 \\ 7 & 1 & -2 \\ 3 & -5 & 11 \\ 1 & 11 & -24 \\ 0 & -38 & 83 \end{array}$$

Así que $(83, 38) = 1 = 11 \cdot 83 + (-24) \cdot 38$.

El número $(a, b)$ puede escribirse de infinitas maneras como combinación lineal de $a$ y $b$: El método matricial nos da una combinación lineal $0 = m_1 a + n_1 b$, que sumado a la igualdad de la penúltima fila nos da $d = (m + km_1)a + (n + kn_1)b$ para cualquier $k \in \mathbb{Z}$.

Dual al concepto de máximo común divisor es el de mínimo común múltiplo:

**Definición 1.5.16.** Un entero positivo $m$ se llama *mínimo común múltiplo* de los enteros no nulos $a$ y $b$ si

1. $m$ es un múltiplo de ambos $a$ y $b$.
2. Cualquier múltiplo de $a$ y $b$ es un múltiplo de $m$.

Usamos la notación $\mathrm{m.c.m.}(a, b)$ o bien $[a, b]$ para el mínimo común múltiplo de $a$ y $b$.

**Teorema 1.5.17.** *El conjunto $I$ de todos los múltiplos de dos enteros no nulos $a$ y $b$ contiene un entero no nulo y es cerrado para la suma y la resta.*

*Dicho conjunto $I$ es de la forma $I = m\mathbb{Z}$, donde $m = \mathrm{m.c.m.}(a, b)$. En particular, dos enteros no nulos cualesquiera tienen un mínimo común múltiplo.*

*Demostración.* El entero $ab$ es distinto de cero y pertenece a $I$. Si $c_1 = q_1 a = p_1 b$ y $c_2 = q_2 a = p_2 b$, entonces $c_1 \pm c_2 = (q_1 \pm q_2)a = (p_1 \pm p_2)b$. Por 1.4.5 tenemos el segundo resultado. □

**Teorema 1.5.18.** *Si $c > 0$, $[ca, cb] = c[a, b]$. También $[a, b](a, b) = ab$.*

*Demostración.* Sean $[ca, cb] = cq$ y $[a, b] = m$. Como $a \mid m$ y $b \mid m$, tenemos que $ac \mid mc$ y $bc \mid mc$, luego $cq \mid mc$ y por tanto $q \mid m$. Por otra parte, $ca \mid cq$, $cb \mid cq$ de donde $a \mid q$, $b \mid q$ y por tanto $m \mid q$. Como ambos son positivos, $m = q$.

Para demostrar la segunda parte podemos suponer que $a, b > 0$ porque $[a, b] = [a, -b]$. Empezamos con el caso especial $(a, b) = 1$. Ahora $[a, b] = ac$. Entonces $b \mid ac$ y como $(a, b) = 1$ necesariamente $b \mid c$, luego $ab \mid ac = [a, b]$. Siempre se cumple que $[a, b] \mid ab$ y como ambos son positivos, son iguales.

En el caso general sea $d = (a, b)$. Tenemos $(a/d, b/d) = 1$. Aplicando el resultado del caso particular se obtiene

$$\left[\frac{a}{d}, \frac{b}{d}\right]\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{a}{d}\frac{b}{d}$$

Multiplicando por $d^2$ obtenemos $[a, b](a, b) = ab$. □

## 1.6. Ecuaciones diofánticas

El estudio de la aritmética elemental de los enteros se divide en varias partes: Divisibilidad y factorización, congruencias, funciones aritméticas y ecuaciones diofánticas. Vamos a introducir estas últimas.

Una *ecuación diofántica* es una ecuación polinómica con coeficientes y raíces enteros. De la misma forma un sistema de ecuaciones diofánticas es un conjunto finito de ecuaciones diofánticas simultáneas. Resolver una ecuación diofántica (o un sistema de ellas) es hallar explícitamente sus raíces enteras.

*Ejemplo* 1.6.1. Consideremos la ecuación $x^2 + y^2 = z^2$. Las soluciones enteras de esta ecuación se llaman *ternas pitagóricas* por motivos obvios. Algunas soluciones conocidas desde antiguo son $(4, 3, 5)$, $(12, 5, 13)$ y $(20, 21, 29)$. Si exigimos que $\text{m. c. d.}(x, y, z) = 1$, la solución general viene dada por $(2uv, u^2 - v^2, u^2 + v^2)$ con $u, v$ de distinta paridad, $u > v$ y $\text{m. c. d.}(u, v) = 1$

*Ejemplo* 1.6.2. Una generalización de la anterior es la *ecuación de Fermat*: $x^n + y^n = z^n$ con $n \geq 3$. El llamado *último teorema de Fermat* establece que esta ecuación no tiene solución entera con $xyz \neq 0$. Para dar una idea de la dificultad de la aritmética, este teorema fué enunciado a mediados del siglo XVII por Fermat y su demostración se remató sólo a finales del siglo XX por Wiles, mas de 300 años después.

Si una ecuación (o sistema) es *determinada*, es decir tiene un número finito de soluciones en $\mathbb{Q}$ o en $\mathbb{R}$, podemos resolverla en uno de estos cuerpos y comprobar sus raíces una a una para ver cuales son enteras. Por ello, las ecuaciones diofánticas interesantes son las *indeterminadas*, que admiten infinitas soluciones en $\mathbb{Q}$ y debemos caracterizar cuales de ellas son enteras.

Vamos a discutir un método para resolver los sistemas diofánticos lineales. El caso mas sencillo es el de una ecuación con dos incógnitas:

$$ax + by = c \tag{1.6.1}$$

**Teorema 1.6.3.** *1. La ecuación 1.6.1 tiene solución si y sólo si* $\text{m. c. d.}(a, b) \mid c$.

*2. Una solución particular de 1.6.1 se obtiene por el algoritmo extendido de Euclides.*

*3. Sea* $d = \text{m. c. d.}(a, b)$ *y sea* $(x_0, y_0)$ *una solución particular de 1.6.1. La solución general* $(x, y)$ *viene dada por*

$$x = x_0 + k\frac{b}{d}, \qquad y = y_0 - k\frac{a}{d}$$

*con* $k \in \mathbb{Z}$ *arbitrario.*

*Demostración.* 1. Supongamos que 1.6.1 tiene una solución $(x_0, y_0)$ y sea $d = \text{m. c. d.}(a, b)$. Entonces

$$c = ax_0 + by_0 = d(\frac{a}{d}x_0 + \frac{b}{d}y_0)$$

y por tanto $d \mid c$.

A la inversa, sea $c = dc_1$. Por el teorema de Bezout existen $m, n \in \mathbb{Z}$ tales que $am + bn = d$. Entonces $(x_0, y_0) = (mc_1, nc_1)$ es una solución de 1.6.1.

2. Por el algoritmo extendido de Euclides encontramos $m, n \in \mathbb{Z}$ tales que $am + bn = d$. El último párrafo del punto anterior termina la demostración.

3. Sea $(x_0, y_0)$ una solución particular, es decir $ax_0 + by_0 = c$. Llamamos $x = x_0 + k\frac{b}{d}$, $y = y_0 - k\frac{a}{d}$ y calculamos $ax + by = a(x_0 + k\frac{b}{d}) + b(y_0 - k\frac{a}{d}) = c$. A la inversa, sea $ax + by = c$. Restando la solución particular tenemos que $(x - x_0)a + (y - y_0)b = 0$. Dividimos por $d = \text{m. c. d.}(a, b)$ y despejamos: $(x - x_0)(a/d) = -(y - y_0)(b/d)$. Como $\text{m. c. d.}(a/d, b/d) = 1$, necesariamente $x - x_0 = k \cdot b/d$ y $-(y - y_0) = h \cdot a/d$. Sustituyendo y simplificando vemos que $k = h$. Finalmente despejando vemos que $x = x_0 + k\frac{b}{d}$ y $y = y_0 - k\frac{a}{d}$

□

Las ideas subyacentes al algoritmo de Euclides pueden aplicarse también para hallar una *solución general en enteros* de cualquier conjunto de ecuaciones lineales con coeficientes enteros. El procedimiento es el siguiente:

1. Buscamos un coeficiente no nulo $c$ de mínimo valor absoluto en el sistema de ecuaciones. Supongamos que este coeficiente aparece en una ecuación que tiene la forma

$$cx_0 + c_1x_1 + \cdots + c_kx_k = d;$$

y por sencillez supongamos $c > 0$.

2. Si $c = 1$, usamos esta ecuación para eliminar la variable $x_0$ de las otras ecuaciones del sistema. Si no quedan mas ecuaciones, el cálculo acaba y hemos obtenido una solución general en términos de las variables no eliminadas.

3. Si $c > 1$, entonces

   - Si $c \mid c_1, \ldots, c \mid c_k$, comprobamos si $c \nmid d$ en cuyo caso no hay solución en enteros.
   - Si $c \mid d$ dividimos ambos miembros por $c$ y eliminamos $x_0$ como en el caso $c = 1$.

4. Si $c > 1$ y existe un $c_i$ no divisible por $c$, dividimos los $c_i$ entre $c$: $c_i = q_ic + r_i$. Introducimos una nueva variable

$$x_0 + q_1x_1 + \cdots + q_kx_k = t;$$

eliminamos la variable $x_0$ de las otras ecuaciones en favor de $t$ y reemplazamos la ecuación original por

$$ct + r_1x_1 + \cdots + r_kx_k = d$$

Este proceso debe terminar ya que cada paso reduce el número de ecuaciones o el valor absoluto del mínimo coeficiente no nulo del sistema.

Cuando se aplica este proceso a la ecuación $ax + by = 1$ para $a, b$ dados, el proceso anterior es esencialmente el algoritmo de Eulides extendido.

*Ejemplo* 1.6.4. Queremos resolver el sistema

$$\begin{aligned} 10w + 3x + 3y + 8z &= 1 \\ 6w - 7x - 5z &= 2 \end{aligned}$$

El coeficiente de menor valor absoluto es 3 que multiplica a $y$ en la primera ecuación y es positivo. Como $3 \nmid 10$, introducimos una nueva variable

$$\lfloor 10/3 \rfloor w + \lfloor 3/3 \rfloor x + \lfloor 3/3 \rfloor y + \lfloor 8/3 \rfloor z = 3w + x + y + 2z = t_1$$

y la usamos para eliminar $y$. La primera ecuación se convierte en

$$(10 \mod 3)w + (3 \mod 3)x + 3t_1 + (8 \mod 3)z = w + 3t_1 + 2z = 1$$

y la segunda ecuación queda igual.

Ahora el coeficiente de $w$ en la primera ecuación es 1. Usamos dicha ecuación para eliminar $w$ y la segunda ecuación se convierte en

$$6(1 - 3t_1 - 2z) - 7x - 5z = 2$$

esto es

$$7x + 18t_1 + 17z = 4$$

.

Introducimos una nueva variable

$$x + 2t_1 + 2z = t_2$$

y eliminamos $x$:

$$7t_2 + 4t_1 + 3z = 4.$$

Introducimos otra variable para eliminar $z$, que tiene el menor coeficiente:

$$2t_2 + t_1 + z = t_3$$

Eliminando $z$ nos queda

$$t_2 + t_1 + 3t_3 = 4$$

y finalmente utilizamos esta ecuación para eliminar $t_2$. Nos quedan dos variables independientes $t_1$ y $t_3$. Sustituyendo hacia atrás en las variables originales obtenemos la solución general:

$$\begin{aligned} w &= 17 - 5t_1 - 14t_3 \\ x &= 20 - 5t_1 - 17t_3 \\ y &= -55 + 19t_1 + 45t_3 \\ z &= -8 + t_1 + 7t_3 \end{aligned}$$

En otras palabras, todas las soluciones enteras $(w, x, y, z)$ del sistema original se obtienen de las última igualdades cuando $t_1$ y $t_2$ recorren independientemente todos los enteros.

El proceso de eliminación de variables descrito (que es reminiscente del método de eliminación de Gauss para sistemas lineales en un cuerpo) es sencillo y directo pero no es el mejor método disponible para este problema. El método que quizá sea el mas elegante y sistemático se basa en la teoría de módulos sobre dominios de ideales principales, teoría general que no se estudia en este curso.

## 1.7. Primos

**Definición 1.7.1.** Un entero $p > 1$ se llama *número primo* si sus únicos divisores son $\pm 1$ y $\pm p$. Un entero $a > 1$ se llama *compuesto* si no es primo.

**Lema 1.7.2** (Euclides). *Un entero $p > 1$ es primo si y sólo si satisface la siguiente propiedad: Si $p \mid ab$ para $a, b \in \mathbb{Z}$, entonces o $p \mid a$ o $p \mid b$.*

*Demostración.* Supongamos que $p$ es un primo y $p \mid ab$. Si $a = 0$ el resultado es claro. Si $a \neq 0$ sabemos que o $(p, a) = p$ o $(p, a) = 1$ porque $(p, a)$ siempre es un divisor de $p$ y $p$ es primo. En el primer caso $p \mid a$ y ya está. En el segundo caso aplicamos el segundo punto del teorema 1.5.8 para mostrar que $p \mid ab$ implica $p \mid b$.

A la inversa, supongamos que $p$ verifica la condición dada. Si $p = ab$ la condición implica que o $p = a$ (ya que $p \mid a$ y $p > a$) o $p = b$ y por tanto $p$ es primo. □

**Teorema 1.7.3** (Teorema fundamental de la aritmética). *Todo entero $a > 1$ se factoriza de manera única como producto de primos en la forma*

$$a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$$

*donde $p_1 < p_2 < \dots < p_n$ y los exponentes $e_1, e_2, \dots, e_n$ son todos positivos.*

*Demostración.* Supongamos que existe algún entero mayor que 1 que no es un producto de números primos. Entonces el conjunto $I$ de todos los enteros positivos que no tienen factorización en primos es no vacío. Por el principio de buena ordenación ese conjunto tiene un primer elemento, sea $b$. Este $b$ no puede ser primo, porque en este caso tendría una factorización en primos. Así que $b = cd$ donde $c, d$ son positivos y menores que $b$. Luego $c, d \notin I$ y por tanto ambos se pueden escribir como producto de primos. Pero entonces $b = cd$ también es un producto de números primos. Luego $I$ es vacío y todo entero mayor que 1 se puede escribir como producto de primos. Además, como la multiplicación de enteros es conmutativa, los factores primos de $b$ pueden ordenarse de la forma deseada.

Si existe un entero mayor que 1 para el que la factorización no es única, por el principio de buena ordenación existe un mínimo entre tales enteros, sea $a$. Sea $a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n} = q_1^{f_1} q_2^{f_2} \dots q_n^{f_m}$ con $p_1 < p_2 < \dots < p_n$ y $q_1 < q_2 < \dots < q_m$. Por el lema de Euclides $q_1 \mid p_k$ para algún $k$ y $p_1 \mid q_j$ para algún $j$. Como todos los $p_i$ y todos los $q_j$ son primos, necesariamente $q_1 = p_k$ y $p_1 = q_j$. Como $q_1 \leq q_j$ y $p_1 \leq p_k$, necesariamente $p_1 = q_1$. Podemos tomar

$$s = \frac{a}{p_1} = \frac{a}{q_1} = p_1^{e_1 - 1} p_2^{e_2} \dots p_n^{e_n} = q_1^{f_1 - 1} q_2^{f_2} \dots q_n^{f_m}$$

Si s=1 entonces $a = p_1$ tiene una factorización única, en contra de la elección de $a$. Si $s > 1$, como $s < a$ y $s$ tiene dos factorizaciones obtenemos otra vez una contradicción con la elección de $a$. □

Podemos considerar a los primos como los elementos a partir de los cuales se obtienen por multiplicación todos los demás números enteros positivos, de la misma forma en que todo número entero positivo se obtiene a partir del 1 mediante suma reiterada.

**Proposición 1.7.4.** *Sean $a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$ y $b = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$ dos enteros positivos descompuestos en factores primos. Entonces $b \mid a$ si y sólo si $f_i \leq e_i$ para todo $i = 1, \dots, n$.*

La factorización en primos permite escribir directamente el máximo común divisor y el mínimo común múltiplo de dos enteros dados:

**Proposición 1.7.5.** *Sean $a, b$ enteros positivos con factorizaciones primas*

$$a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n} \quad y \quad b = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$$

*con* $e_i, f_i \geq 0$ *para todo* $i$.

*Para cada* $i$ *sean* $g_i = \min(e_i, f_i)$ *y* $h_i = \max(e_i, f_i)$. *Entonces*

$$\text{m. c. d.}(a, b) = p_1^{g_1} p_2^{g_2} \dots p_n^{g_n}$$
$$\text{m. c. m.}(a, b) = p_1^{h_1} p_2^{h_2} \dots p_n^{h_n}$$

*Demostración.* La demostración se sigue inmediatamente del teorema fundamental de la aritmética y las definiciones de máximo común divisor y mínimo común múltiplo. □

Para números pequeños probablemente es mas fácil usar sus factorizaciones primas para hallar el máximo común divisor y el mínimo común múltiplo. Pero para números grandes hallar su factorización en primos es muy lento, aún usando algoritmos sofisticados sobre ordenadores potentes. En contraste, el algoritmo de Euclides es mucho mas rápido y eficiente para calcular el máximo común divisor de grandes números.

*Ejemplo* 1.7.6. Calculamos una vez mas $(126, 35)$. Descomponemos en factores primos: $126 = 2^1 \cdot 3^2 \cdot 5^0 \cdot 7^1$ y $35 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1$. Así que $(126, 35) = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 = 7$ y $[126, 35] = 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 630$

Si conocemos la factorización de un entero es fácil listar todos sus divisores: Si $a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$ entonces $b$ es un divisor de $a$ si y sólo si $b = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$ con $f_i \leq e_i$ para todo $i$. Así que podemos listar todos los divisores de $a$ disminuyendo sistemáticamente los exponentes de cada uno de sus factores primos.

**Teorema 1.7.7** (Euclides)**.** *Existen infinitos primos*

*Demostración.* Supongamos que sólo hubiese un número finito de primos, sean $p_1, p_2, \dots, p_n$. Formamos el número $a = p_1 p_2 \dots p_n + 1$. Por el teorema 1.7.3 existe un divisor primo de $a$, sea $p$. Este debe estar en la lista así que $p \mid (p_1 p_2 \dots p_n)$, luego $p \mid (a - p_1 \dots p_n) = 1$. Pero un primo no puede dividir a 1. □

## 1.8. Congruencias

Para muchos problemas aritméticos, la información importante está en los restos obtenidos al dividir por un entero fijo $n$. Como sólo son posibles los $n$ restos diferentes $0,\ 1,\ \cdots,\ n-1$, pueden producirse considerables simplificaciones. Para valores pequeños de $n$ es posible incluso utilizar el método de prueba y error.

*Ejemplo* 1.8.1. Un teorema de Lagrange establece que todo entero positivo puede escribirse como suma de cuatro cuadrados. Vamos a ver que si $n$ es un entero positivo que al dividirlo por 8 da de resto 7, no puede expresarse como suma de tres cuadrados, por lo que el teorema de Lagrange es el mejor posible:

Sea $n = a^2 + b^2 + c^2$. Al dividir ambos miembros por 8 los restos deben ser iguales. Por la proposición 1.8.6 podemos calcular el resto de $a^2 + b^2 + c^2$ calculando los restos de $a$, $b$ y $c$, elevándolos al cuadrado y sumándolos (y dividiendo por 8 si es necesario). Los posibles valores para $a^2, b^2, c^2$ son $0, 1, 4$. Para comprobar los posibles valores del resto de $a^2 + b^2 + c^2$ sólo tenemos que sumar tres de tales valores. Un estudio de todos los casos muestra que no podemos obtener 7como resto de $a^2 + b^2 + c^2$. Luego si $n$ da de resto 7 al dividirlo por 8, no puede ser suma de tres cuadrados.

La técnica de prueba y error puede usarse para ver que una ecuación polinómica no tiene raíces enteras:

*Ejemplo* 1.8.2. Sea $f(x) = x^3 + 3412x^2 - 1235x + 678443$. Supongamos que existiese un $n \in \mathbb{Z}$ tal que $f(n) = 0$. Al tomar los restos módulo 2 nos queda $n^3 + n + 1 = 0$. Pero $n^3 + n + 1$ es impar para cualquier valor de $n$, luego $f(n) \neq 0$ para todo valor de $n$.

Una situación familiar en la que efectuamos los cálculos tras dividir por un valor fijo es en la suma de horas, donde el entero fijo es 12. Las reglas de los signos es hacer el cálculo con los restos al dividir por 2. Gauss introdujo la notación de congruencia que simplifica los cálculos de este tipo:

**Definición 1.8.3.** Sea $n$ un entero positivo. Los enteros $a$ y $b$ se llaman *congruentes módulo $n$* si tienen el mismo resto al dividirlos por $n$. Esto se denota por $a \equiv b \pmod{n}$ o $a \equiv b \mod n$

Si utilizamos el algoritmo de la división para escribir $a = nq + r$ donde $0 \leq r < n$ entonces $r = n \cdot 0 + r$. Es inmediato de la definición precedente que $a \equiv r \pmod{n}$. En particular cualquier entero es congruente módulo $n$ a uno de los enteros $0, 1, 2, \ldots, n-1$.

La definición 1.8.3 proporciona la mejor visión intuitiva del concepto de congruencia, pero en casi todas las demostraciones es mas fácil utilizar la siguiente caracterización, que permite usar los hechos sobre divisibilidad que ya hemos estudiado:

**Proposición 1.8.4.** *Sean $a, b, n \in \mathbb{Z}$ con $n > 0$. Entonces $a \equiv b \pmod{n}$ si y sólo si $n \mid (a - b)$.*

*Demostración.* Si $a \equiv b \pmod{n}$, entonces $a = nq_1 + r$ y $b = nq_2 + r$. Despejando el resto tenemos $r = a - nq_1 = b - nq_2$. Trasponiendo términos $a - b = n(q_1 - q_2)$, luego $n \mid (a - b)$.

A la inversa sea $n \mid (a - b)$, así que $a - b = nq$. Por el algoritmo de la división $b = nq_1 + r$ con $0 \leq r < n$. Sumando ambas igualdades tenemos que $a = n(q + q_1) + r$, luego los restos de dividir $a$ por $n$ y $b$ por $n$ son iguales y por tanto $a \equiv b \pmod{n}$. □

Esta proposición nos dice que $a \equiv b \pmod{n}$ si y sólo si $a - b = nq$ para algún entero $q$, lo que podemos escribir como $a = b + nq$. Esta observación proporciona un método muy útil de reemplazar una congruencia por una ecuación diofántica.

**Proposición 1.8.5.** *La relación $a \equiv b \pmod{n}$ es una relación de equivalencia.*

**Proposición 1.8.6.** *Sea $n > 0$ un entero. Cualesquiera $a, b, c, d \in \mathbb{Z}$ verifican las siguientes propiedades:*

1. *Si $a \equiv c \pmod{n}$ y $b \equiv d \pmod{n}$, entonces $a + b \equiv c + d \pmod{n}$, $a - b \equiv c - d \pmod{n}$ y $ab \equiv cd \pmod{n}$.*
2. *Si $a + c \equiv a + d \pmod{n}$ entonces $c \equiv d \pmod{n}$. Si $ac \equiv ad \pmod{n}$ y $(a, n) = 1$ entonces $c \equiv d \pmod{n}$.*

*Demostración.* Sean $a \equiv c \pmod{n}$ y $b \equiv d \pmod{n}$. Entonces $n \mid (a - c)$ y $n \mid (b - d)$. Sumando tenemos que $n \mid ((a + b) - (c + d))$ y restando $n \mid ((a - b) - (c - d))$. También tenemos que $n \mid (a - c)b = ab - cb$ y $n \mid c(b - d) = cb - cd$. Sumando tenemos $n \mid (ab - cd)$.

Sea ahora $a + c \equiv a + d \pmod{n}$. Entonces $n \mid ((a + c) - (a + d)) = c - d$. Si $ac \equiv ad \pmod{n}$ tenemos que $n \mid (ac - ad) = a(c - d)$ y como $(a, n) = 1$, se sigue que $n \mid (c - d)$. □

Las principales consecuencias de esta proposición son:

1. Podemos sustituir cualquier entero de la congruencia por un entero congruente. Por ejemplo para mostrar que $99^2 \equiv 1 \pmod{100}$ lo mas fácil es sustituir 99 por $-1$ y calcular $(-1)^2 = 1$.
2. Podemos sumar o restar el mismo entero a ambos miembros de una congruencia.
3. Podemos multiplicar ambos miembros de una congruencia por el mismo entero.
4. Hay que tener mucho cuidado al simplificar o dividir ambos miembros de la congruencia por el mismo entero $a$: Sólo puede hacerse cuando $(a, n) = 1$. Por ejemplo $30 \equiv 6 \pmod{8}$ pero al dividir ambos miembros por 6 tenemos $5 \equiv 1 \pmod{8}$, lo cual es falso. Pero al dividir por 3 tenemos $10 \equiv 2 \pmod{8}$ lo que es correcto porque $(3, 8) = 1$.

5. Cualquier ecuación diofántica puede convertirse a una congruencia módulo $n$ simplemente cambiando el signo $=$ por $\equiv$ y cualquier término congruente a 0 puede sencillamente omitirse. Este proceso se conoce como *reducción módulo n*. Por ejemplo la ecuación $x^3+5x^2+6x-11=0$ se convierte en $x^3+x^2+1\equiv 0 \pmod 2$.

*Ejemplo* 1.8.7. La proposición 1.8.6 muestra que para calcular el resto de dividir $a+b$ o $ab$ por $n$ podemos calcular los restos de dividir $a$ y $b$ entre $n$ y sumarlos o multiplicarlos, dividiendo otra vez por $n$ si es necesario. Por ejemplo, $101 \equiv 5 \pmod 8$ y $142 \equiv 6 \pmod 8$, así que $101 \cdot 142 \equiv 5 \cdot 6 \equiv 6 \pmod 8$.

*Ejemplo* 1.8.8. Vamos a calcular las potencias de 2 módulo 7. En vez de calcular cada potencia y entonces dividir por 7, reducimos módulo 7 en cada paso del cálculo:

$$\begin{aligned} 2^2 &\equiv 4 \pmod 7, \\ 2^3 \equiv 2^2 2 &\equiv 4 \cdot 2 \equiv 1 \pmod 7, \\ 2^4 \equiv 2^3 2 &\equiv 1 \cdot 2 \equiv 2 \pmod 7, \\ 2^5 \equiv 2^4 2 &\equiv 2 \cdot 2 \equiv 4 \pmod 7 \end{aligned}$$

Tal como hemos hecho los cálculos, está claro que las potencias se repiten. De hecho como sólo hay un número finito de posibles restos módulo $n$, las potencias módulo $n$ de cualquier entero siempre acaban repitiéndose.

**Proposición 1.8.9.** *Sean $a, n \in \mathbb{Z}$ con $n > 1$. Existe un entero $b$ tal que $ab \equiv 1 \pmod n$ si y sólo si $(a, n) = 1$.*

*Demostración.* Supongamos que existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod n$. Luego $ab = 1 + nq$ con $q \in \mathbb{Z}$. Esto puede reescribirse como una combinación lineal $ab - nq = 1$. Luego $(a, n) = 1$.

A la inversa sea $(a, n) = 1$. Entonces existen $b, t \in \mathbb{Z}$ tales que $ab + tn = 1$. Reduciendo módulo $n$ obtenemos $ab \equiv 1 \pmod n$. □

## 1.9. Sistemas de ecuaciones en congruencias

Vamos a presentar un estudio sistemático de ecuaciones lineales en congruencias. En muchos aspectos resolver congruencias es como resolver ecuaciones sobre los enteros. Pero existen algunas diferencias: Una ecuación lineal en una incógnita sobre los enteros tiene como máximo una solución, mientras que $2x \equiv 2 \pmod 4$ tiene dos soluciones: $x \equiv 1 \pmod 4$ y $x \equiv 3 \pmod 4$. También puede ocurrir que no existan soluciones, por ejemplo $3x \equiv 2 \pmod 6$ no las tiene. Así que el primer paso es obtener un teorema para determinar si existe o no alguna solución. Naturalmente para $a, b, n$ pequeños, las soluciones de $ax \equiv b \pmod n$ se pueden encontrar probando todas las posibilidades.

La proposición 1.8.9 muestra que la congruencia

$$ax \equiv 1 \pmod n$$

tiene solución si y sólo si $(a, n) = 1$. De hecho la demostración de dicha proposición muestra que se obtiene una solución utilizando el algoritmo extendido de Euclides para expresar $1 = ab + nq$ con $b, q \in \mathbb{Z}$.

**Definición 1.9.1.** Dos soluciones $r$ y $s$ a la congruencia $ax \equiv b \pmod n$ son distintas módulo $n$ si $r$ y $s$ no son congruentes módulo $n$.

**Teorema 1.9.2.** *La congruencia $ax \equiv b \pmod n$ tiene solución si y sólo si $b$ es divisible por $d = \text{m. c. d.}(a, n)$. Si $d \mid b$, existen $d$ soluciones distintas módulo $n$ y estas soluciones son congruentes módulo $n/d$.*

*Demostración.* La congruencia $ax \equiv b \pmod{n}$ tiene solución si y sólo si existen enteros $s, q \in \mathbb{Z}$ tales que $as = b + nq$ o lo que es lo mismo, $as + (-q)n = b$. Así que existe una solución si y sólo si se puede expresar $b$ como combinación lineal de $a$ y $n$. Pero tales combinaciones son precisamente los múltiplos de $d$.

Sea ahora $d \mid b$ y sea $m = n/d$. Sean $x_1, x_2$ soluciones de la congruencia $ax \equiv b \pmod{n}$, así que $ax_1 \equiv ax_2 \pmod{n}$. Luego $n \mid (ax_1 - ax_2)$ y por tanto $n \mid d(x_1 - x_2)$ y $m = (n/d) \mid (x_1 - x_2)$ con lo que $x_1 \equiv x_2 \pmod{m}$.

A la inversa, si $x_1 \equiv x_2 \pmod{m}$ entonces $m \mid (x_1 - x_2)$, $n = dm \mid d(x_1 - x_2)$. Como $d \mid a$ podemos concluir que $n \mid a(x_1 - x_2)$ o lo que es lo mismo, que $ax_1 \equiv ax_2 \pmod{n}$.

Las distintas soluciones están entre los restos $0, 1, \ldots, n-1$. Dada una de las soluciones, todas las otras se hallan sumando múltiplos de $n/d$, lo que nos da un total de $d$ soluciones distintas. □

Vamos a describir un algoritmo para resolver congruencias lineales de la forma

$$ax \equiv b \pmod{n} \tag{1.9.1}$$

1. Calculamos $d = (a, n)$. Si $d \nmid b$, la ecuación no tiene solución.
2. Si $d \mid b$ escribimos la congruencia 1.9.1 como una ecuación diofántica $ax = b + qn$.
3. Ya que $d$ es un divisor común de $a$, $b$ y $n$ podemos tomar $a = da_1$, $b = db_1$ y $n = dn_1$. Dividiendo la anterior ecuación por $d$ nos queda $a_1 x = b_1 + qn_1$.
4. La congruencia 1.9.1 es por tanto equivalente a
$$a_1 x \equiv b_1 \pmod{n_1}$$
donde ahora $(a_1, n_1) = 1$.
5. Por la proposición 1.8.9 hallamos un entero $c$ tal que $ca_1 \equiv 1 \pmod{n_1}$. Multiplicando ambos miembros por $c$ obtenemos
$$x \equiv cb_1 \pmod{n_1}$$
6. Finalmente, ya que la congruencia original era módulo $n$, debemos dar nuestra respuesta módulo $n$. La solución módulo $n_1$ determina $d$ soluciones distintas módulo $n$: $x \equiv b_1 c + kn_1$ con $k = 0, \ldots, d-1$.

*Ejemplo* 1.9.3 (Congruencias lineales homogéneas). Vamos a considerar el caso especial de una ecuación homogénea lineal

$$ax \equiv 0 \pmod{n}$$

En este caso siempre existe una solución, $x \equiv 0 \pmod{n_1}$, pero puede que no sea la única.

En el segundo paso de la solución obtenemos $a_1 x \equiv 0 \pmod{n_1}$. Ya que $(a_1, n_1) = 1$, por la proposición 1.8.6 podemos cancelar $a_1$ y nos queda $x \equiv 0 \pmod{n_1}$, luego las $d$ soluciones son $x \equiv 0, n_1, 2n_1, \ldots, (d-1)n_1 \pmod{n}$.

Por ejemplo la congruencia $28x \equiv 0 \pmod{48}$ tiene cuatro soluciones distintas módulo 48: $x \equiv 0, 12, 24, 36 \pmod{48}$

*Ejemplo* 1.9.4. Para resolver la congruencia $60x \equiv 90 \pmod{105}$ primero calculamos $D = (60, 105) = 15$. Como $15 \mid 90$, la ecuación tiene solución. Dividiendo por $d$ obtenemos la ecuación

$$4x \equiv 6 \pmod{7} \tag{1.9.2}$$

Buscamos un entero $c$ tal que $4c \equiv 1 \pmod{7}$, a saber $c = 2$. Multiplicamos ambos miembros de 1.9.2 por $c$ y obtenemos $8x \equiv 12 \pmod{7}$, que se reduce a $x \equiv 5 \pmod{7}$.

La ecuación original tiene pues quince soluciones:

$$x \equiv 5 + 7k \pmod{105} \text{ con } k = 0, 1, \ldots 14$$

## 1.10. Teorema chino de los restos

Vamos a estudiar ahora la resolución de sistemas de ecuaciones en congruencias. Empezamos por el caso de dos congruencias:

**Teorema 1.10.1.** *Dos congruencias simultáneas*

$$x \equiv a \pmod{m} \qquad x \equiv b \pmod{n} \tag{1.10.1}$$

*tienen solución si y sólo si* $a \equiv b \pmod{(m,n)}$. *En este caso la solución es única módulo* $[m,n]$.

*Demostración.* De la primera congruencia de 1.10.1 se sigue que $x = a + mt$. Sustituyendo en la segunda obtenemos que $t$ debe verificar la ecuación $a + mt \equiv b \pmod{n}$ lo que es lo mismo que $mt \equiv (b-a) \pmod{n}$. Hemos visto anteriormente que esta ecuación tiene solución si y sólo si $d = (m,n)$ divide a $(b-a)$, y en ese caso es equivalente a la congruencia

$$\frac{m}{d}t \equiv \frac{b-a}{d} \pmod{\frac{n}{d}}$$

Sea $t_0$ una solución particular de esta congruencia. La solución general es

$$t \equiv t_0 \pmod{\frac{n}{d}}$$

así que $t = t_0 + u(n/d)$ con $u \in \mathbb{Z}$. La solución general de la congruencia original es

$$x \equiv a + m\left(t_0 + \frac{n}{d}u\right) = x_0 + u\frac{mn}{d}$$

o sea $x \equiv x_0 \pmod{[m,n]}$. □

*Ejemplo* 1.10.2. Vamos a resolver el sistema

$$x \equiv 5 \pmod{11}, \qquad x \equiv 3 \pmod{23}$$

La primera congruencia dice que $x = 5 + 11t$. Sustituyendo en la segunda obtenemos la ecuación $5 + 11t \equiv 3 \pmod{23}$, es decir $11t \equiv -2 \pmod{23}$. La única solución de esta última es $t \equiv 4 \pmod{23}$. La forma general de $t$ es pues $t = 4 + 23u$. Sustituido en la expresión para $x$ tenemos que $x = 5 + 11(4 + 23u) = 49 + (11 \cdot 23)u$. Luego la solución general del sistema propuesto es $x \equiv 49 \pmod{11 \cdot 23}$.

*Ejemplo* 1.10.3. El sistema

$$x \equiv 7 \pmod{42} \qquad x \equiv 15 \pmod{51}$$

no tiene solución porque $d = (42, 51) = 3$ y $7 \not\equiv 15 \pmod{3}$.

*Ejemplo* 1.10.4. Sea el sistema

$$x \equiv 3 \pmod{14} \qquad x \equiv 7 \pmod{16}$$

Aquí $d = (14, 16) = 2$ y $3 \equiv 7 \pmod{2}$, luego existe una solución única módulo $[14, 16] = 112$. Realizando los cálculos vemos que la solución es $x \equiv 87 \pmod{112}$.

Cuando los módulos $m$ y $n$ de 1.10.1 son primos relativos existe otro método para obtener la solución del sistema: Por el algoritmo extendido de Euclides determinamos $u, v \in \mathbb{Z}$ tales que $um + vn = 1$. Entonces $x = avn + bum$ es una solución. En efecto $vn \equiv 1 \pmod{m}$ y $um \equiv 1 \pmod{n}$. Por tanto $x = avn + bum \equiv a(vn) \equiv a \pmod{m}$ y $x \equiv b(um) \equiv b \pmod{n}$.

*Ejemplo* 1.10.5. Vamos a resolver el sistema

$$x \equiv 7 \pmod 8 \qquad x \equiv 3 \pmod 5$$

El algoritmo extendido de Euclides nos dice que $2 \cdot 8 + (-3) \cdot 5 = 1$. Luego la solución general del sistema propuesto es

$$x = 7 \cdot (-3) \cdot 5 + 3 \cdot 2 \cdot 8 = -105 + 48 = -57 \equiv 23 \pmod{40}$$

Consideramos ahora el caso general, donde hay $r \geq 2$ congruencias simultáneas. Necesitamos un resultado que conecta máximos comunes divisores y mínimos comunes múltiplos:

**Lema 1.10.6.** *Para $a, b, c \in \mathbb{Z}$ arbitrarios se verifican las propiedades distributivas:*

$$(a, [b, c]) = [(a, b), (a, c)]$$
$$[a, (b, c)] = ([a, b], [a, c])$$

*Demostración.* Sea $p$ un primo arbitrario y sean $p^i, p^j, p^k$ las máximas potencias de $p$ que dividen respectivamente a $a, b, c$. Como el enunciado es simétrico para $b$ y $c$, podemos tomar $j \geq k$. Entonces la máxima potencia de $p$ que divide a $[b, c]$ es $p^j$ y el exponente de la máxima potencia de $p$ que divide a $(a, [b, c])$ es mín$(i, j)$. Por otra parte los exponentes de las máximas potencias de $p$ que dividen a $(a, b)$ y $(a, c)$ son respectivamente mín$(i, j)$ y mín$(i, k)$. Como $j \geq k$, tenemos que mín$(i, j) \geq$ mín$(i, k)$. Luego el exponente de la máxima potencia de $p$ que divide a $[(a, b), (a, c)]$ es mín$(i, j)$. Así que $(a, [b, c])$ y $[(a, b), (a, c)]$ tienen la misma descomposición en primos y por tanto son iguales.

La demostración de la segunda propiedad es análoga. □

**Teorema 1.10.7.** *Un sistema de r congruencias simultáneas*

$$x \equiv a_i \pmod{m_i} \quad i = 1, 2, \ldots, r \tag{1.10.2}$$

*tiene solución si y sólo si para todo par de índices i, j se verifica*

$$a_i \equiv a_j \pmod{(m_i, m_j)} \tag{1.10.3}$$

*y en este caso la solución es única módulo $M_r = [m_1, \ldots, m_r]$.*

*Demostración.* En primer lugar hay que observar que si las congruencias 1.10.2 tienen solución, dos cualesquiera de ellas también la tienen, así que por el teorema 1.10.1, deben verificarse las condiciones 1.10.3.

Demostramos por inducción que estas condiciones son suficientes: El teorema 1.10.1 es el caso $r = 2$. Supongamos que el resultado es cierto para $r - 1$ congruencias. Con esta hipótesis existe una solución

$$x_0 \equiv a_i \pmod{m_i} \quad i = 1, 2, \ldots, r - 1 \tag{1.10.4}$$

y cualquier otra solución $x$ debe ser de la forma $x \equiv x_0 \pmod{M_{r-1}}$, $M_{r-1} = [m_1, \ldots, m_{r-1}]$. Para que $x$ sea solución de todas las ecuaciones 1.10.2 debe satisfacer además $x \equiv a_r \pmod{m_r}$. Por el teorema 1.10.1 concluimos que este conjunto de congruencias tiene solución sólo cuando

$$x_0 \equiv a_r \pmod{(M_{r-1}, m_r)} \tag{1.10.5}$$

y que en este caso existe una solución única módulo $[M_{r-1}, m_r] = M_r$.

Queda por comprobar que el $x_0$ hallado verifica las condiciones 1.10.5. Por el lema 1.10.6 tenemos que

$$(M_{r-1}, m_r) = ([m_1, \ldots, m_{r-1}], m_r) = [(m_1, m_r), \ldots, (m_{r-1}, m_r)]$$

por lo que el sistema de congruencias 1.10.5 es equivalente al sistema

$$x_0 \equiv a_r \pmod{(m_i, m_r)}, \qquad i = 1, 2, \ldots, r - 1$$

Pero estas últimas se derivan fácilmente de las hipótesis. □

*Ejemplo* 1.10.8. En *Disquisitiones Arithmeticae* de Gauss aparece el siguiente sistema:

$$x \equiv 17 \pmod{504}, \quad x \equiv -4 \pmod{35}, \quad x \equiv 33 \pmod{16}$$

Al resolver las dos primeras congruencias obtenemos $x \equiv 521 \pmod{2520}$ y combinando esta con la tercera de las congruencias dadas el resultado final es $x \equiv 3041 \pmod{5040}$

*Ejemplo* 1.10.9. Muchos entretenimientos matemáticos pertenecen al tipo de problemas que se resuelven por congruencias simultáneas. Existen diversos manuscritos medievales que contienen colecciones de problemas populares y muchos de estos problemas, con pequeñas variantes, se pueden reconocer casi todas las semanas en las revistas actuales. Un ejemplo:

*Una anciana va al mercado con un canasto de huevos y un caballo pisa el canasto y rompe los huevos. El jinete acepta pagar los daños y pregunta cuántos huevos ha roto. Ella no recuerda el número exacto, pero cuando los tomaba de dos en dos sobraba un huevo. Lo mismo sucedía cuando los cogía en grupos de tres, cuatro, cinco o seis respectivamente; pero cuando los agrupaba de siete en siete no sobraba ninguno. ¿Cual es el menor número de huevos que había en el canasto?* En términos matemáticos esto significa que

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

donde $x$ es el número de huevos. Las cinco primeras condiciones pueden combinarse para dar $x \equiv 1$ mód 60. Resolviendo con la última de las congruencias dadas obtenemos la solución $x \equiv 301 \pmod{420}$, así que el mínimo número de huevos que contenía el cesto es 301.

El caso especial en que los módulos de las congruencias 1.10.2 son primos relativos dos a dos ocurre en muchas aplicaciones. De acuerdo con el teorema 1.10.7 existe una solución única a estas congruencias módulo el producto de todos los $m_i$. Gauss introdujo un procedimiento especial, usado previamente por Euler, para determinar la solución. Pero el método es aún mas antiguo y aparece en las obras de varios matemáticos. La primera fuente conocida es la *Aritmética* del autor chino Sun-Tse, alrededor del siglo I de nuestra era, y la fórmula resultante se conoce como *teorema chino de los restos*.

Empezamos formando el producto $M = m_1 m_2 \dots m_r$. Al dividir $M$ entre $m_i$ el cociente

$$\frac{M}{m_i} = m_1 \dots m_{i-1} m_{i+1} \dots m_r \tag{1.10.6}$$

es divisible por todos los módulos excepto por $m_i$, con el que es primo relativo. Por tanto podemos resolver para todo $i$ la congruencia lineal

$$b_i \frac{M}{m_i} \equiv 1 \pmod{m_i}$$

y podemos enunciar:

**Teorema 1.10.10** (Teorema chino de los restos)**.** *Sea dado un sistema de congruencias 1.10.2 donde los módulos $m_i$ son primos relativos dos a dos. Para cada i se determina un $b_i$ que satisfazga la congruencia lineal 1.10.6. La solución del sistema de congruencias es*

$$x \equiv a_1 b_1 \frac{M}{m_1} + a_2 b_2 \frac{M}{m_2} + \dots + a_r b_r \frac{M}{m_r} \pmod{M} \tag{1.10.7}$$

*Demostración.* La verificación es sencilla: $m_i$ divide a todos los $M/m_j$ salvo a $M/m_i$ así que

$$x \equiv a_i b_i \frac{M}{m_i} \equiv a_i \pmod{m_i}$$

□

*Ejemplo* 1.10.11. El ejemplo dado por Sun-Tse corresponde a las tres congruencias

$$x \equiv 2 \pmod 3 \quad x \equiv 3 \pmod 5 \quad x \equiv 2 \pmod 7$$

Aquí $M = 3 \cdot 5 \cdot 7 = 105$ y

$$\frac{M}{m_1} = 35, \quad \frac{M}{m_2} = 21, \quad \frac{M}{m_3} = 15$$

El conjunto de congruencias lineales

$$35b_1 \equiv 1 \pmod 3 \quad 21b_2 \equiv 1 \pmod 5 \quad 15b_3 \equiv 1 \pmod 7$$

tiene las soluciones $b_1 = 2, b_2 = 1, b_3 = 1$ así que de acuerdo con la fórmula 1.10.7 la solución es

$$x \equiv 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 \equiv 233 \pmod{105}$$

En la fórmula 1.10.7 para calcular los multiplicadores $b_i M/m_i$ sólo hacen falta los números $m_i$. Por tanto, si hay que resolver varios sistemas de congruencias con los mismos módulos, la expresión 1.10.7 es particularmente adecuada porque hay que calcular los multiplicadores sólo una vez.

Las congruencias son una herramienta muy útil en cuestiones de calendario, tales como la determinación de la Pascua, el día de la semana de una fecha concreta y problemas parecidos. Gauss ilustra el teorema chino de los restos con el problema de encontrar los años que tienen un cierto período respecto a los ciclos solar y lunar y al índice romano. Anteriormente el matemático indio Brahmagupta (siglo VII) trató problemas similares respecto a los ciclos planetarios.

*Ejemplo* 1.10.12. Leonardo discute en el *Liber Abaci* la siguiente cuestión: *Se le pide a alguien que piense un número. Entonces se le piden los restos del número al dividirlo por* 5, 7 *y* 9 *y con esta información se adivina el número pensado*.

Vamos a denotar como $x$ al número desconocido y por $a_1, a_2, a_3$ a los tres restos de forma que

$$x \equiv a_1 \pmod 5 \quad x \equiv a_2 \pmod 7 \quad x \equiv a_3 \pmod 9$$

Los módulos son primos relativos y $M = 5 \cdot 7 \cdot 9 = 315$,

$$\frac{M}{m_1} = 63, \quad \frac{M}{m_2} = 45, \quad \frac{M}{m_3} = 35$$

Las congruencias lineales

$$63b_1 \equiv 1 \pmod 5, \quad 45b_2 \equiv 1 \pmod 7, \quad 35b_1 \equiv 1 \pmod 9$$

tienen las soluciones $b_1 = 2, b_2 = 5, b_3 = 8$ así que la fórmula 1.10.7 nos da

$$x \equiv 126a_1 + 225a_2 + 280a_3 \pmod{315}$$

De esta expresión obtenemos $x$ según los restos conocidos $a_1, a_2, a_3$. La solución es única sólo si se exige que el número requerido sea menor que 315.

*Ejemplo* 1.10.13. (*Regiomontanus*). Hallar un número $x$ tal que

$$x \equiv 3 \pmod{10}, \quad x \equiv 11 \pmod{13}, \quad x \equiv 15 \pmod{17}$$

*Ejemplo* 1.10.14. (*Euler*). Hallar un número $x$ tal que

$$x \equiv 3 \pmod{11}, \quad x \equiv 5 \pmod{19}, \quad x \equiv 10 \pmod{29}$$

Concluimos con una observación que se aplicará después: Supongamos que al resolver un problema hay que determinar un número $x$ que para un módulo $m_1$ tiene $s_1$ valores admisibles

$$x \equiv a_1, \ldots, a_{s_1} \pmod{m_1}$$

y para otro módulo $m_2$ hay $s_2$ valores admisibles

$$x \equiv b_1, \ldots, b_{s_2} \pmod{m_2}$$

Cuando $(m_1, m_2) = 1$ cada valor $m_i$ puede combinarse con cada valor $b_j$, así que en total hay $s_1 s_2$ soluciones módulo $m_1 m_2$. Esta observación puede generalizarse a $r$ módulos primos relativos dos a dos.

*Ejemplo* 1.10.15. Vamos a resolver la ecuación

$$x^2 \equiv 1 \pmod{40}$$

Es inmediato comprobar que esa ecuación equivale al sistema

$$x^2 \equiv 1 \pmod{5} \qquad x^2 \equiv 1 \pmod{8}$$

Como los módulos son pequeños, por prueba y error vemos que las soluciones de estas ecuaciones son

$$x \equiv 1, 4 \pmod{5} \qquad x \equiv 1, 3, 5, 7 \pmod{8}$$

El algoritmo de Euclides nos dice que $(-3) \cdot 5 + 2 \cdot 8 = 1$. El teorema chino de los restos nos dice que $x \equiv 16a_i - 15b_j \pmod{40}$ donde $a_i = 1, 4$ y $b_j = 1, 3, 5, 7$. Después de reducir módulo 40 obtenemos todas las soluciones:

$$x \equiv 1, 11, 21, 31, 9, 19, 29, 39 \pmod{40}$$

Resulta bastante mas dificil resolver congruencias del tipo $a_k x^k + \cdots + a_1 x + a_0 \equiv 0 \pmod{n}$. Utilizando el teorema chino de los restos el problema se reduce a resolver congruencias módulo $p^e$ para factores primos de $n$. Y las soluciones módulo $p^e$ se determinan a partir de las soluciones módulo primo $p$. Si el primo $p$ es pequeño, estas últimas pueden obtenerse por prueba y error, sencillamente sustituyendo sucesivamente $0, 1, \ldots, p-1$ en la congruencia. Además podemos utilizar el teorema de Fermat que hay mas adelante para reducir el problema a uno donde el grado del polinomio sea menor que $p$

## 1.11. Los anillos $\mathbb{Z}_n$

Al trabajar con congruencias hemos visto que en cualquier cálculo los números congruentes son intercambiables. Vamos a formalizar este punto de vista. Consideramos como un ente individual a toda una clase de enteros congruentes y trabajamos con estas clases igual que con los enteros ordinarios. El motivo de introducir la notación que viene a continuación es permitirnos usar nuestra experiencia con los enteros ordinarios como una guía para trabajar con congruencias. Muchas de las propiedades de la aritmética entera se verifican también en la aritmética de congruencias. La excepción mas notable es que el producto de dos clases de congruencia no nulas puede ser cero.

**Definición 1.11.1.** San $a, n \in \mathbb{Z}$ con $n > 0$. Llamamos *clase de congruencia de a módulo n* al conjunto de todos los enteros que son congruentes con $a$ módulo $n$. La denotamos por $a + n\mathbb{Z}$ o por $[a]_n$:

$$a + n\mathbb{Z} = [a]_n = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$$

El conjunto de todas las clases de congruencia módulo $n$ se llama *conjunto de los enteros módulo n* y se representa por $\mathbb{Z}_n$.

Nótese que $[a]_n = [b]_n$ si y sólo si $a \equiv b \pmod{n}$. Cuando el módulo $n$ está claro del contexto suprimimos el índice y escribimos sólo $[a]$.

Una clase de congruencia puede designarse de infinitas maneras. Por ejemplo, $[5]_3 = [8]_3 = [-1]_3 = \ldots$. A un elemento $a$ de la clase $[a]_n$ le llamamos *representante* de la clase. Toda clase de congruencia $[a]_n$ tiene un único representante $r$ tal que $0 \leq r < n$ (a saber, $r$ es el resto de dividir $a$ entre $n$). Esto demuestra que hay exactamente $n$ clases de congruencias módulo $n$ distintas. Por ejemplo, los elementos de $\mathbb{Z}_3$ son

$$[0]_3 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$
$$[1]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$
$$[2]_3 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

Cada entero pertenece exactamente a una clase de congruencia módulo 3, porque el resto de dividir por 3 es único. En general, cada entero pertenece a una única clase de congruencia módulo $n$, luego

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

El conjunto $\mathbb{Z}_2$ tiene exactamente dos elementos: $[0]_2$ es el conjunto de los enteros pares y $[1]_2$ es el de los impares. Con esta notación las conocidas reglas "par + par = par", "impar + par = impar", "impar + impar = par" se expresan como $[0]_2 + [0]_2 = [0]_2$, $[1]_2 + [0]_2 = [1]_2$, $[1]_2 + [1]_2 = [0]_2$. De la misma forma, las reglas "par × par = par", "impar × par = par", "impar × impar = impar" se expresan como $[0]_2 \cdot [0]_2 = [0]_2$, $[1]_2 \cdot [0]_2 = [0]_2$, $[1]_2 \cdot [1]_2 = [1]_2$. Estas reglas pueden resumirse dando una tabla de adición y una tabla de multiplicación para $\mathbb{Z}_n$:

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| · | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

En estas tablas hemos utilizado una simplificación habitual al tratar con congruencias: Omitimos el subindice e incluso los corchetes y escribimos $a$ en lugar de $[a]_n$.

Para $\mathbb{Z}_n$ se introducen una suma y un producto análogos:

Dados $[a]_n, [b]_n \in \mathbb{Z}_n$ definimos

$$[a]_n + [b]_n = [a+b]_n$$
$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

**Proposición 1.11.2.** *Sea $n$ un entero positivo y sean $a, b, a_1, b_1 \in \mathbb{Z}$ tales que $[a]_n = [a_1]_n$ y $[b]_n = [b_1]_n$. Entonces $[a+b]_n = [a_1 + b_1]_n$ y $[a \cdot b]_n = [a_1 \cdot b_1]_n$.*

Esta proposición dice que la suma y multiplicación de clases de congruencia están bien definidas, es decir que son independientes de los representantes que escojamos en cada clase.

Las leyes asociativas y conmutativas de la suma y el producto, la ley distributiva y la existencia de neutros son válidas en $\mathbb{Z}_n$. Si $[a]_n + [b]_n = [0]_n$, la clase $[b]_n$ se llama *opuesta* a la clase $[a]_n$. El opuesto de una clase es único. Es fácil ver que de hecho el opuesto de $[a]_n$ es $[-a]_n$. Se denota por $-[a]_n = [-a]_n$. En general no se verifican las leyes de integridad y cancelativa.

**Definición 1.11.3.** Sean $[a]_n, [b]_n \in \mathbb{Z}_n$ con $[b]_n \neq [0]_n$ y $[a]_n[b]_n = [0]_n$. Entonces $[a]_n$ se llama *divisor de cero*.

**Proposición 1.11.4.** *Sea $[a]_n$ un no divisor de cero y sea $[a]_n[b]_n = [a]_n[c]_n$. Entonces $[b]_n = [c]_n$.*

**Definición 1.11.5.** Sean $[a]_n, [b]_n \in \mathbb{Z}_n$ tales que $[a]_n[b]_n = [1]_n$. Entonces decimos que $[a]_n, [b]_n$ son elementos *invertibles* o *unidades* de $\mathbb{Z}_n$ y que $[b]_n$ es un *inverso* de $[a]_n$. Denotamos $[b]_n = [a]_n^{-1}$.

Obsérvese que si $[a]$ es invertible, no puede ser divisor de cero.

**Proposición 1.11.6.** *Sea $n$ un entero positivo.*

1. *La clase $[a]_n$ tiene un inverso multiplicativo en $\mathbb{Z}_n$ si y sólo si $(a, n) = 1$.*
2. *Un elemento no nulo de $\mathbb{Z}_n$ o es invertible o es divisor de cero.*

*Demostración.* 1. Supongamos que $[a]$ tiene un inverso $[a]^{-1} = [b]$. Entonces $[ab] = [a][b] = [1]$, luego $ab \equiv 1 \pmod{n}$, lo que implica que $ab = qn + 1$ para algún entero $q$. O sea que $ab + (-q)n = 1$ y por tanto $(a, n) = 1$.

A la inversa sea $(a, n) = 1$. Entonces existen $b, c \in \mathbb{Z}$ tales que $ab + cn = 1$. Reduciendo módulo $n$ vemos que $ab \equiv 1 \pmod{n}$ y por tanto $[a][b] = [ab] = [1]$.

2. Sea $[a] \neq 0$ lo que equivale a $n \nmid a$. Si $(a, n) = 1$ entonces$[a]$ tiene un inverso, En otro caso $(a, n) = d > 1$ Como $d \mid a$ y $d \mid n$ existen enteros $k, b$ tales que $n = kd$ y $a = bd$. Entonces $[k] \neq [0]$ pero $[a][k] = [ak] = [bdk] = [bn] = [0]$, lo que muestra que $[a]$ es un divisor de cero.

□

**Corolario 1.11.7.** *Para un módulo $n > 0$ las siguientes condiciones son equivalentes:*

1. *El número $n$ es primo.*
2. *$\mathbb{Z}_n$ no tiene divisores de cero no nulos.*
3. *Todo elemento no nulo de $\mathbb{Z}_n$ tiene un inverso multiplicativo.*

La demostración de la proposición 1.11.6 muestra que si $(a, n) = 1$ entonces podemos calcular el inverso multiplicativo de $a$ utilizando el algoritmo extendido de Euclides:

*Ejemplo* 1.11.8. Para hallar $[11]^{-1} \in \mathbb{Z}_{16}$ realizamos el siguiente cálculo:

$$\begin{array}{ccc} 16 & 0 & 1 \\ 11 & 1 & 0 \\ 5 & -1 & 1 \\ 1 & 3 & -2 \\ 0 & -16 & 11 \end{array}$$

luego $11 \cdot 3 + 16 \cdot (-2) = 1$, lo que muestra que $[11]^{-1} = [3]$.

Hay otros dos métodos para hallar el inverso multiplicativo de $[a]_n$ en $\mathbb{Z}_n$: Si el módulo $n$ es pequeño, a veces es mas corto hacerlo por prueba y error. La otra forma es calculando las potencias sucesivas de $[a]$. Si $(a, n) = 1$, entonces $[a]$ no es divisor de cero en $\mathbb{Z}_n$ y por tanto ninguna potencia $[a]^k$ puede ser cero. El conjunto $\{[a], [a]^2, [a]^3, \dots\}$ tiene menos de $n$ elementos distintos, luego en algún punto debe repetirse. Sean $k < m$ tales que $[a]^m = [a]^k$. Entonces $[a]^{m-k} = [a]^0 = [1]$. Esto muestra que en la primera repetición debe ser $k = 0$ y por tanto $[a]^m = [1]$. De aquí vemos que $[a]^{m-1} = [1]$.

*Ejemplo* 1.11.9. Volvamos a calcular $[11]_{16}^{-1}$. Para ello listamos las potencias sucesivas de $[11]_{16}$:

$$\begin{aligned} [11]^2 &= [-5]^2 = [25] = [9] \\ [11]^3 &= [11]^2[11] = [9][11] = [99] = [3] \\ [11]^4 &= [11]^3[11] = [3][11] = [33] = [1] \end{aligned}$$

luego $[11]^{-1} = [11]^3 = [3]$.

Podemos ahora estudiar ecuaciones en $\mathbb{Z}_n$. La congruencia lineal $ax \equiv b \pmod{n}$ puede verse ahora como una ecuación lineal $[a]_n[x]_n = [b]_n$ en $\mathbb{Z}_n$. Si $[a]_n$ tiene inverso, esta ecuación tiene solución única $[x] = [a]_n^{-1}[b]_n$. Nótese que sin la noción de clase de congruencia tenemos que modificar la afirmación de unicidad para decir que si $x_0$ es una solución de $ax \equiv b \pmod{n}$, también lo es $x_0 + qn$ para cualquier entero $q$.

Vamos a ver finalmente dos teoremas que permiten rebajar el grado de las ecuaciones polinómicas en $\mathbb{Z}_n$.

**Definición 1.11.10.** Sea $n$ un entero positivo. El número de enteros positivos menores o iguales que $n$ y que son primos relativos con $n$ se denota $\varphi(n)$. Esta función se llama *función $\varphi$ de Euler* o *función tociente*.

Nótese que $\varphi(1) = 1$. Para $n > 1$ el valor de $\varphi(n)$ puede obtenerse de la factorización en primos:

**Lema 1.11.11.** *Sea $n = p^e$. Entonces $\varphi(n) = p^e - p^{e-1} = n(1 - 1/p)$*

*Demostración.* Un entero $m$ es primo relativo con $p^e$ si y sólo si es primo con $p$. Como $p$ es primo, esto quiere decir que *$m$ no es* primo relativo con $p^e$ si y sólo si es un múltiplo de $p$. El número de todos los enteros entre 1 y $p^e$ es $p^e$. El número de múltiplos de $p$ entre 1 y $p^e$ es $p^{e-1}$. Restando obtenemos el resultado del lema. □

**Lema 1.11.12.** *Sean $m, n$ enteros positivos primos relativos. Entonces $\varphi(mn) = \varphi(m)\varphi(n)$.*

*Demostración.* Definimos una aplicación $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ (el producto cartesiano mediante $f([a]_{mn}) = ([a]_m, [a]_n)$. Por el teorema chino de los restos, $f$ es una biyección. Es fácil comprobar que $f[a]_{mn}[b]_{mn}) = f([a]_{mn})f([b]_{mn})$. En particular $[a]_{mn}$ será invertible si y sólo si lo son ambas $[a]_m$ y $[a]_n$. Pero para cualquier $k$ la clase $[a]_k$ es invertible si y sólo si $(a, k) = 1$. Así que por restricción, $f$ establece una biyección entre los enteros positivos menores o iguales que $mn$ primos relativos con $mn$ con el conjunto de pares de enteros positivos donde la primera componente sea menor o igual que $m$ y primo relativo con $m$ y la segunda sea menor o igual que $n$ y primo relativo con $n$. Contando estos pares obtenemos el resultado buscado. □

**Proposición 1.11.13.** *Sea $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ la factorización en primos de $n$. Entonces*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$$

*Demostración.* Consecuencia inmediata de los dos lemas anteriores:

$$\varphi(n) = \varphi(p_1^{e_1}) \dots \varphi(p_k^{e_k})$$

por el lema 1.11.12 y aplicando a cada factor el lema 1.11.11 obtenemos el resultado final. □

*Ejemplo* 1.11.14. Las fórmulas de la proposición anterior nos dicen que

$$\varphi(10) = 10\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4$$

y que

$$\varphi(36) = 36\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12$$

**Definición 1.11.15.** El conjunto de unidades de $\mathbb{Z}_n$, es decir el conjunto de clases $[a]_n$ con $(a, n) = 1$ se denota por $\mathbb{Z}_n^\times$.

**Proposición 1.11.16.** *El conjunto $\mathbb{Z}_n^\times$ es cerrado para la multiplicación.*

*Demostración.* Es inmediato comprobar que $([a][b])^{-1} = [b]^{-1}[a]^{-1}$. □

El conjunto $\mathbb{Z}_n^\times$ tiene $\varphi(n)$ elementos. El siguiente teorema debe verse como un resultado sobre potencias de elementos de $\mathbb{Z}_n^\times$:

**Teorema 1.11.17** (Euler). *Sea $(a,n) = 1$. Entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

*Demostración.* En el conjunto $\mathbb{Z}_n$ existen $\varphi(n)$ elementos que tienen un representante primo relativo a $n$. Sean estos $\{a_1, \ldots, a_{\varphi(n)}\}$. Las clases representadas por $\{aa_1, \ldots, aa_{\varphi(n)}\}$ son todas distintas porque $(a,n) = 1$. Como cada producto $aa_i$ es primo relativo con $n$, tenemos un representante de cada una de las clases de partida. Por tanto

$$a_1 a_2 \ldots a_{\varphi(n)} \equiv (aa_1)(aa_2)\ldots(aa_{\varphi(n)}) \equiv a^{\varphi(n)} a_1 a_2 \ldots a_{\varphi(n)} \pmod{n}$$

Ya que el producto $a_1 a_2 \ldots a_{\varphi(n)}$ es primo relativo con $n$ podemos simplificarlo y nos queda la congruencia

$$1 \equiv a^{\varphi(n)} \pmod{n}$$

□

**Corolario 1.11.18** (Teorema de Fermat). *Sea $p$ un primo. Entonces $a^p \equiv a \pmod{p}$ para todo entero $a$.*

*Demostración.* Si $p \mid a$, entonces $a^p \equiv 0 \equiv a \pmod{p}$. Si $p \nmid a$ entonces $(a,p) = 1$ y el teorema de Euler nos dice que $a^{\varphi(p)} \equiv 1 \pmod{p}$. Pero $\varphi(p) = p-1$. Multiplicando ambos miembros por $a$ tenemos el resultado buscado. □

El teorema de Fermat proporciona un *criterio de número compuesto*: Sea $n$ un número del que queremos averiguar si es primo o compuesto. Tomamos un $a$ primo relativo con $n$ (por ejemplo, $a = 2$) y calculamos $b \equiv a^{n-1} \pmod{n}$. Si $b \neq 1$, el número $n$ es compuesto. Pero si $b = 1$ no sabemos si el número $n$ es primo o compuesto. Naturalmente podemos probar con otra base $a$ distinta, pero aunque para varios $a$ se verifique que $a^{n-1} \equiv 1 \pmod{n}$, no podemos concluir que $n$ sea primo. De hecho existen números $n$ tales que $a^{n-1} \equiv 1 \pmod{n}$ para *todo* $a$ primo relativo con $n$. Tales números se llaman *números de Carmichael*, hay 2163 entre 1 y $25 \cdot 10^9$ y el mas pequeño es $561 = 3 \cdot 11 \cdot 17$.

El criterio anterior se puede afinar (véase cualquier libro sobre teoría de números), pero aún los criterios mejorados no son concluyentes (existen números compuestos que los pasan). Para finalizar vamos a ver un *criterio de primalidad* de interés teórico, aunque poco práctico.

**Lema 1.11.19.** *Sea $p$ un primo. Entonces $a^2 \equiv 1 \pmod{p}$ si y sólo si $a \equiv 1 \pmod{p}$ o $a \equiv -1 \pmod{p}$*

*Demostración.* La hipótesis es que $p \mid (a^2 - 1) = (a-1)(a+1)$. Por ser $p$ primo tiene que dividir a uno de los factores. □

En términos de clases de restos este lema dice que $[a]_p^{-1} = [a]_p$ si y sólo si $[a]_p = \pm[1]$.

**Teorema 1.11.20** (Teorema de Wilson). *Un entero positivo $p$ es primo si y sólo si $(p-1)! \equiv -1 \pmod{p}$*

*Demostración.* Supongamos que $(p-1)! \equiv -1 \pmod{p}$. Entonces existe un entero $q$ tal que $qp - (p-1)! = 1$, así que $\text{m. c. d.}(p,(p-1)!) = 1$ y $p$ no es divisible por ningún entero menor que $p$ y mayor que 1 (todos ellos dividen a $(p-1)!$. Luego $p$ es primo.

A la inversa sea $p$ primo distinto de 2 (el caso $p = 2$ se comprueba fácilmente). Multiplicamos todas las clases $[1]_p \cdot [2]_p \cdots [p-1]_p$. Por el lema 1.11.19, para cada clase $[a]_p$ en este producto, salvo la primera y la última, también $[a]_p^{-1}$ está en el producto. Y el producto vale $[a]_p[a]_p^{-1} = 1$. Luego $[(p-1)!]_p = [p-1]_p = [-1]_p$. Pero este es el resultado buscado. □

## 1.12. Ejercicios

**Ejercicio 1.1.** Demostrar:

1. $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.
2. $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.
3. $\sum_{i=1}^{n} i^3 = [\frac{n(n+1)}{2}]^2$.
4. $\sum_{i=1}^{n} i^5 + \sum_{i=1}^{n} i^7 = 2[\frac{n(n+1)}{2}]^4$.
5. $\sum_{i=1}^{n}(2i-1) = n^2$.
6. $2^n \leq n!$ para todo $n \geq 4$.
7. $2^n > n^3$ para todo $n \geq 10$.

**Ejercicio 1.2.** Demostrar que para todo entero $n \geq 1$ se verifica:

i) $\overline{(A_1 \cup A_2 \cup ... \cup A_n)} = \overline{A_1} \cap \overline{A_2} \cap ... \cap \overline{A_n}$

ii) $\overline{(A_1 \cap A_2 \cap ... \cap A_n)} = \overline{A_1} \cup \overline{A_2} \cup ... \cup \overline{A_n}$

**Ejercicio 1.3.** La sucesión de Fibonacci está definida por recurrencia de la siguiente forma:

$$\begin{cases} a_0 = 0 \\ a_1 = 1 \\ a_n = a_{n-1} + a_{n-2}, \quad \text{para } n \geq 2. \end{cases}$$

1. Calcular los 10 primeros términos de la sucesión.
2. Probar que
$$a_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

**Ejercicio 1.4.** Vamos a demostrar por inducción que $\sum_{i=1}^{n} i = \frac{(n-1)(n+2)}{2}$. Para ello supongamos que el resultado es cierto para $n$ y veamos que ocurre para $n+1$.

$$\begin{aligned} \sum_{i=1}^{n+1} i = & \quad \sum_{i=1}^{n} i + (n+1) = \frac{(n-1)(n+2)}{2} + (n+1) = \\ = & \quad \frac{n^2+n-2}{2} + \frac{2n+2}{2} = \frac{n^2+3n}{2} = \\ = & \quad \frac{n(n+3)}{2} = \frac{(n+1)-1)((n+1)+2)}{2}. \end{aligned}$$

¿Es correcta esta demostración?

**Ejercicio 1.5.** ¿Qué es erróneo en la demostración del siguiente teorema?

**Teorema 1.12.1.** *Cualquier conjunto $\{a_1, a_2, ..., a_n\}$ tiene la propiedad de que todos sus elementos son iguales.*

*Demostración.* La demostración se hace por inducción sobre $n$.

Para $n = 1$ el resultado es cierto pues cualquier conjunto $\{a_1\}$ tiene la propiedad requerida.

Supongamos el resultado cierto para $n-1$ y consideremos el conjunto $\{a_1, a_2, ..., a_n\}$. La hipótesis de inducción aplicada al subconjunto $\{a_1, ..., a_{n-1}\}$ da $a_1 = a_2 = ... = a_{n-1}$ y aplicada al subconjunto $\{a_2, ..., a_n\}$ da $a_2 = ... = a_n$. Entonces $a_1 = a_2 = ... = a_{n-1} = a_n$ como se quería demostrar. □

**Ejercicio 1.6.** Denotamos

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

Probar que

$$\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}.$$

Utilizando esta igualdad, probar por inducción

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

**Ejercicio 1.7.** Probar por inducción que para todo número par $k$, el resto de dividir $2^k$ entre 3 es 1.

**Ejercicio 1.8.** Probar por inducción que para todo número impar $k$, el resto de dividir $2^k$ entre 3 es 2.

**Ejercicio 1.9.** Para cada una de las siguientes parejas de enteros $(a, b)$, calcula el máximo común divisor $d = \text{m. c. d.}(a, b)$ y enteros $u, v$ que satisfagan la relación de Bezout, esto es, tales que $d = ua + vb$

$$\begin{array}{ll} a = -99\,, & b = 17, \\ a = 6643\,, & b = 2873, \\ a = -7655\,, & b = 1001 \\ a = 24230\,, & b = 586. \end{array}$$

**Ejercicio 1.10.** Demuestra que para todo $n \in \mathbb{N}$:

a) $3^{2n} - 2^n$ es divisible por 7, b) $3^{2n+1} - 2^{n+2}$ es divisible por 7,

c) $3^{2n+2} + 2^{6n+1}$ es divisible por 11, d) $3 \cdot 5^{2n+1} + 2^{3n+1}$ es divisible por 17.

**Ejercicio 1.11.** Demostrar que si $a$ y $b$ son enteros primos relativos y $n$ es un entero divisible por $a$ y por $b$ entonces lo es por $ab$.

**Ejercicio 1.12.** Demuestra que si $3 \mid a^2 + b^2$, entonces $3 \mid a$ y $3 \mid b$.

**Ejercicio 1.13.** Demuestra que si $5 \mid a^2 + b^2 + c^2$, entonces $5 \mid a$ o $5 \mid b$ o $5 \mid c$.

**Ejercicio 1.14.** Sean $a, b, c$ enteros no nulos. Demostrar que $(a, b) = 1$ y $(a, c) = 1$ si y solo si $(a, [b, c]) = 1$.

**Ejercicio 1.15.** Para n natural calcula: $\text{m. c. d.}(n, n^2)$, $\text{m. c. d.}(n, n+1)$ y $\text{m. c. d.}(n, n+2)$.

**Ejercicio 1.16.** Resolver las ecuaciones diofánticas

$$60x + 36y = 12, \qquad 35x + 6y = 8, \qquad 12x + 18y = 11.$$

**Ejercicio 1.17.** Se dispone de 4050 euros para gastar en bolígrafos de 10 euros y en plumas de 46 euros. Calcular cuantos bolígrafos y plumas se pueden comprar si se quiere el menor número posible de bolígrafos.

**Ejercicio 1.18.** Definimos la sucesión siguiente:
$F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ para $n \geq 2$.

1. Demuestra que $\text{mcd}(F_n, F_{n+1}) = 1$ y $\text{mcd}(F_n, F_{n+2}) = 1$ para $n \geq 0$.

2. Calcula todas las soluciones enteras de la ecuación $F_7 \cdot x - F_5 \cdot y = 3$.

**Ejercicio 1.19.** Factorizar en primos cada uno de los siguientes números y, usando estas factorizaciones, calcular el máximo común divisor y el mínimo común múltiplo de cada una de las parejas que puedas formar con ellos: 6643, 2873, 4148, 252.

**Ejercicio 1.20.** Demostrar que entre $-|b|$ y $|b|$ no hay múltiplos de $b$ salvo el cero.

**Ejercicio 1.21.** Demostrar que cualquier entero $n > 1$ ó es primo ó tiene un factor primo $\leq \sqrt{n}$. ¿Cuantos primos hay entre 27270 y 27280? ¿y entre 4900 y 4905?.

**Ejercicio 1.22.** Demostrar que cualquier producto de números de la forma $4n + 1$ es otra vez de esa forma. Deducir que hay infinitos primos de la forma $4n - 1$.

**Ejercicio 1.23.** (Antiguo problema chino) Tres agricultores dividieron equitativamente el arroz que habían cultivado en común. Para venderlo fueron a mercados diferentes, donde se usaban diferentes medidas de peso, además todos ellos usaron carretas en las que podían transportar un máximo de 1000 libras. En el primer mercado la medida era de 11 libras, en el segundo de 14 y en el tercero de 15 libras. Cada agricultor vendió todo lo que pudo en medidas enteras y cuando volvieron al hogar, el primero llevaba 5 libras de arroz, el segundo 6 y el tercero 4. ¿Cuanto arroz habían cultivado entre los tres?

**Ejercicio 1.24.** (Antiguo problema chino) Cuatro cuadrillas de albañiles emprenden la construcción de un dique, cada una se compromete a ejecutar el mismo número de jornadas de trabajo y todas ellas trabajarán al menos una jornada completa, siendo el número de jornadas completas de trabajo inferior a 1500. La primera de las cuadrillas consta de 2 hombres, la segunda de tres, la tercera de 7 y la cuarta de 25. Completando el trabajo en jornadas completas de cada cuadrilla, al final quedó un día de trabajo para un hombre de la primera cuadrilla, para dos de la segunda y para cinco de la tercera y cuarta. ¿Cuantos fueron los días de trabajo empleados en construir el dique?

**Ejercicio 1.25.** Un grupo de 12 ladrones decidieron robar un cofre lleno de monedas de oro, que según un informe fidedigno contenía entre 2000 y 3000 monedas. El día del robo, uno de ellos resultó apresado, los 11 restantes decidieron repartir las monedas a partes iguales. Al hacer el reparto resultó que sobraron 8 monedas que decidieron darían a María, la mujer del ladrón apresado. María, no contenta con el reparto, delató a los dos ladrones que lo habían propuesto, después de lo cual quedaron 9 ladrones en libertad que volvieron a repartirse el botín. En este caso solo sobraron 2 monedas, que en su momento darían a María. Indignada María con el comportamiento de los compinches de su marido, decidió acabar con todos ellos y quedarse con todo el botín. Para ello, colocó una bomba en el lugar de reunión de la banda, desafortunadamente para María, la bomba hizo explosión cuando solo se encontraban 4 ladrones en el local. Los que quedaron, volvieron a decidir repartir el botín a partes iguales y dar a María la única moneda que sobraba del reparto. Esto indignó aún más a María, que mediante intrigas consiguió que disputaran los ladrones entre ellos, muriendo 3 en la disputa. Los dos que quedaron con vida repartieron el botín a partes iguales y no sobró moneda alguna. ¿que cantidad de monedas tenía el cofre?

**Ejercicio 1.26.** Encontrar todas las soluciones del sistema de congruencias:

$$x \equiv 3 \pmod 5; x \equiv -2 \pmod 4; x \equiv 1 \pmod 7$$

**Ejercicio 1.27.** Antonio, Pepe y Juan son tres campesinos que principalmente se dedican al cultivo de la aceituna. Este año la producción de los olivos de Antonio fue tres veces la de los de Juan y la de Pepe cinco veces la de los de Juan. Los molinos a los que estos campesinos llevan la aceituna, usan recipientes de 25 litros el de Juan, 7 litros el de Antonio y 16 litros el de Pepe. Al envasar el aceite producido por los olivos de Juan sobraron 21 litros, al envasar el producido por Antonio sobraron 3 litros y al envasar el producido por Pepe sobraron 11 litros. Sabiendo que la producción de Juan está entre 1000 y 2000 litros ¿cuál fue la producción de cada uno de ellos?. Definimos la sucesión siguiente:

**Ejercicio 1.28.** Calcular la menor capacidad posible de un depósito de agua sabiendo que a un depósito de doble capacidad le ha faltado un litro para poder ser llenado con garrafas de 5 litros, mientras que a uno de quíntuple capacidad también le ha faltado un litro tanto si se llenaba con garrafas de 7 litros como de 11 litros.

**Ejercicio 1.29.** En la finca de Juan todos los años se consume la misma cantidad de fertilizante, que siempre viene en un camión de menos de 2 toneladas de capacidad. En los tres últimos años Juan ha utilizado, para envasar el fertilizante, sacos de 75, 56 y 143 kilogramos respectivamente. El primer año al envasar el fertilizante sobraron 21 Kg, el segundo 45 y el tercero 77. ¿Qué cantidad de fertilizante consume Juan anualmente? En la finca vecina de la de Juan se han utilizado, también en los últimos tres años, los mismos sacos que Juan y al envasar su fertilizante en estos sacos han sobrado las mismas cantidades que a Juan, sin embargo en esta finca se necesitan más de un camión para transportar su fertilizante. ¿Que cantidad mínima de fertilizante se usa en la finca vecina de la de Juan?

**Ejercicio 1.30.** Calcular el resto de dividir $279^{323}$ entre 17. Análogamente, si se divide $320^{207}$ entre 13.

**Ejercicio 1.31.** Demostrar las reglas del 2,3,5 y 11 para la división.

**Ejercicio 1.32.** Calcular las dos últimas cifras de $3^{3^{100}}$.

## 1.13. Aritmética entera usando GAP

### 1.13.1. Cociente y resto

Dados dos enteros $a$ y $b$, el resto de dividir $a$ entre $b$ se puede calcular usando el comando `mod`.

```
gap> -3 mod 5;
2
```

Y el cociente se puede calcular de la siguiente forma.

```
gap> (-3-(-3 mod 5))/5;
-1
```

Si GAPescribimos $-3/5$, el resultado es un racional, y si usamos el comando `Int`, obtenemos la parte entera de dividir de ese racional, que no es precisamente lo que buscamos.

```
gap> Int((-3)/5);
0
```

### 1.13.2. Máximo común divisor y mínimo común múltiplo. Coeficientes de Bézout

El máximo común divisor de dos enteros (o más) puede ser calculado con el comando `Gcd`, y su mínimo común múltiplo con el comando `Lcm`.

```
gap> Gcd(3,-5);
1
gap> Lcm(3,-5);
15
```

Si queremos conseguir los coeficientes de Bézout, podemos usar el comando `GcdRepresentation` (entre las muchas posibilidades que da GAPpara esto).

```
gap> GcdRepresentation(3,-5);
[ 2, 1 ]
gap> GcdRepresentation(10,15,18);
[ 7, -7, 2 ]
```

### 1.13.3. Ecuaciones diofánticas

Como ya sabemos, una vez resuelto el problema de encontrar los coeficientes de Bézout de un máximo común divisor de dos enteros, tenemos también solución para resolver una ecuación diofántica. Lo único que tenemos que comprobar es si el término independiente es divisible por el máximo común divisor de los coeficientes, y luego multiplicar los coeficientes de Bézout por el factor apropiado para conseguir una solución particular.

Si queremos resolver $10x + 25y = 45$, hacemos lo siguiente.

```
gap> Gcd(10,25);
5
#vemos si 45 es divisible por 5
gap> 45 mod 5;
0
```

```
#calculamos 45 entre 5
gap> 45/last2;
9
#multiplicamos el resultado por los coeficientes de Bézout
gap> last*GcdRepresentation(10,25);
[ -18, 9 ]
#comprobamos el resultado
gap> last*[10,25];
45
```

### 1.13.4. Primos

Para factorizar un entero en producto de primos podemos usar el comando `Factors`.

```
gap> Factors(100);
[ 2, 2, 5, 5 ]
```

También podemos saber si un número es primo usando el comando `IsPrime`.

```
gap> IsPrime(10);
false
gap> IsPrime(7);
true
```

`Primes` es una lista que contiene los primos menores que mil.

```
#el tercer primo
gap> Primes[3];
5
#los primeros cuarenta primos
gap> Primes{[1..40]};
[ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,
  59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113,
  127, 131, 137, 139, 149, 151, 157, 163, 167, 173 ]
```

También podemos hacer un filtro de una lista para ver qué elementos en ella son primos.

```
gap> Filtered([1..300],IsPrime);
[ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,
  59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113,
  127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181,
  191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251,
  257, 263, 269, 271, 277, 281, 283, 293 ]
```

### 1.13.5. Congruencias

Gracias a los coeficientes de Bézout también podemos resolver cualquier congruencia del tipo $ax \equiv b$ mód $m$, con $a$, $b$ y $m$ enteros ($m \neq 0$).

Sea la congruencia $60x \equiv 90 \mod 105$.

```
gap> Gcd(60,105);
15
#dividimos todo por 15
gap> [60,90,105]/15;
[ 4, 6, 7 ]
#buscamos el inverso de 4 módulo 7
#(me quedo con el coeficiente de Bézout de 4)
gap> GcdRepresentation(4,7)[1];
2
#la solución particular es por tanto
gap> 2*6 mod 7;
5
```

Si lo que queremos es resolver un sistema de congruencias de la forma

$$x \equiv a_1 \mod m_1,$$
$$\ldots x \equiv a_n \mod m_n,$$

entonces podemos usar el comando `ChineseRem`, cuyo primer argumento es la lista de módulos y el segundo una lista (con la misma longitud) de residuos.

Así, para resolver $x \equiv 3 \mod 14$, $x \equiv 7 \mod 16$ hacemos lo siguiente.

```
gap> ChineseRem([14,16],[3,7]);
87
```

### 1.13.6. Los anillos $\mathbb{Z}_n$

La función `ZmodnZ` nos permite definir en GAPel anillo de enteros módulo el argumento entero que le pasemos.

```
gap> A:=ZmodnZ(10);
(Integers mod 10)
```

El uno de un anillo (el elemento neutro del producto) se calcula con el comando `One`.

```
gap> uno:=One(A);
ZmodnZObj( 1, 10 )
```

Podemos hacer operaciones elementales en ese anillo, como calcular inversos, sumar elementos.

```
gap> 1/(3*uno);
ZmodnZObj( 7, 10 )
gap> Int(last);
7
gap> 2*uno+6/3*uno;
ZmodnZObj( 4, 10 )
```

Si un elemento no tiene inverso, devuelve `fail`.

```
gap> 1/(2*uno);
ZmodnZObj( fail, 10 )
gap> Int(last);
fail
```

También podemos usar la función `Inverse`.

```
gap> Inverse(2*uno);
fail
gap> Inverse(3*uno);
ZmodnZObj( 7, 10 )
```

Y extraer así el conjunto de unidades de $\mathbb{Z}_{10}$.

```
gap> Filtered([1..9],n->Inverse(n*uno)<>fail);
[ 1, 3, 7, 9 ]
```

Aunque esto lo podíamos haber hecho usando la función `PrimeResidues`.

```
gap> PrimeResidues(10);
[ 1, 3, 7, 9 ]
```

La función $\varphi$ de Euler (función tociente) se expresa como `Phi` en GAP.

```
gap> Phi(10);
4
```

Para $n$ positivo, en GAPexiste el comando `Z(n)` que nos proporciona el menor elemento primitivo de $\mathbb{Z}_n$ (el menor residuo módulo $n$ que genera al grupo multiplicativo de $\mathbb{Z}_n$).

```
gap> uno:=One(Z(7));
Z(7)^0
gap> 2*uno+3*uno;
Z(7)^5
gap> Int(last);
5
gap> 2/3*uno;
Z(7)
gap> Int(last);
3
gap> 1/3*uno;
Z(7)^5
gap> last*2;
Z(7)
```

## 1.14. Aritmética entera con MATHEMATICA

### 1.14.1. Funciones predefinidas en MATHEMATICA

La función `Quotient[a,b]` devuelve el cociente de la división de $a$ por $b$.
Ejemplo:

```
In[1]:= Quotient[6,5]
Out[1]= 1

In[2]:= Quotient[8,-3]
Out[2]= -3
```

La función `GCD[a,b]` devuelve el máximo común divisor de $a$ y $b$.
Ejemplo

```
In[3]:= GCD[234,56]
Out[3]= 2
```

La función `ExtendedGCD[a,b]` (Algoritmo de Euclides extendido) devuelve `{d,{u,v}}` con $d$ el máximo común divisor de $a$ y $b$ y $u$ y $v$ (coeficientes de Bezout) enteros tales que $d = ua + vb$.
Ejemplo

```
In[4]:= ExtendedGCD[234,56]
Out[4]= {2,{-11,46}}
```

La función `LCM[a,b]` devuelve el mínimo común múltiplo de a y b.
Ejemplo

```
In[5]:= LCM[24,56]
Out[5]= 168
```

La función `Mod[a,n]` calcula el resto de la división de $a$ entre $n$ (comparar con la función `Resto[a,b]` definida mas abajo)
Ejemplo

```
In[6]:= Mod[8,-3]
Out[6]= -1

In[7]:= Mod[8,-4]
Out[7]= 0
```

### 1.14.2. Definición de funciones

- Para indicar que $x$ es una variable escribiremos `x_`.
- Si queremos definir una función $f$ que depende de las variables $x$ e $y$ escribiremos `f[x_,y_]:=`.

Ejemplo: Definir la función $f(x, y) = 2x - 4y^2$ y calcular $f(3, 5)$:

```
In[8]:= f[x_,y_]:=2 x-4 y^2

In[9]:= f[3,5]
Out[9]= -94
```

**Definir una función para calcular el resto de la división de $a$ por $b$**

Si definimos

```
In[10]:= Resto[a_,b_]:=a-b*Quotient[a,b]
```

y calculamos

```
In[11]:= Resto[8,3]
Out[11]= 2
```

obtenemos el resto esperado 2. Pero si calculamos

```
In[12]:= Resto[8,-3]
Out[12]= -1
```

obtenemos $-1$ que no es el resto esperado en la división euclídea. Ajustamos mejor nuestra definición de resto poniendo

```
In[13]:= nresto[a_,b_]:=If[b>0 , a-b*Quotient[a,b], a-b*Quotient[a,b]-b]
```

y tenemos

```
In[14]:= nresto[8,-3]
Out[14]= 2
```

que es el resto esperado en la división euclídea, pero

```
In[15]:= nresto[8,-4]
Out[15]= 4
```

que, de nuevo, no es el resto esperado en la división euclídea. Afinamos mas la definición:

```
In[16]:= NResto[a_,b_]:=a-b*Quotient[a,b]/;b>0
NResto[a_,b_]:=NResto[a,-b]
```

Obtenemos

```
In[18]:= NResto[8,-3]
Out[18]= 2

In[19]:= NResto[8,-4]
Out[19]= 0
```

que si es el resto esperado. Análogamente,

```
In[20]:= NResto[7,-2]
Out[20]= 1
```

### 1.14.3. Manejo de Listas

Una lista en MATHEMATICAse introduce poniendo sus elementos entre llaves y separados por comas.
Ejemplo: Para definir una lista con los elementos $a$, $b$, $c$ y elegir el $b$ se procede así:

```
In[21]:= L:={a,b,c}

In[22]:= L[[2]]
Out[22]= b
```

Para introducir la lista con elementos $a,\ b,\ c$ y $\{x, y, z\}$ y elegir el elemento $y$ de esta lista:

```
In[23]:= L:={a,b,c,{x,y,z}}

In[24]:= L[[4,2]]
Out[24]= y
```

Cómo definir una función `NIF[x]` para calcular la letra del NIF:
Para realizar este ejercicio hay que saber que la letra del NIF correspondiente al número $x$ es la letra que ocupa el lugar $r + 1$ de la lista

$$\{T, R, W, A, G, M, Y, F, P, D, X, B, N, J, Z, S, Q, V, H, L, C, K, E\}$$

donde $r$ es el resto de dividir $x$ entre 23. Consideramos entonces la lista

```
In[25]:= L:={"T","R","W","A","G","M","Y","F","P","D","X","B","B","J","Z","S","Q","V","H","L","C","K","E
```

y definimos

```
In[26]:= NIF[x_]:=L[[Mod[x,23]+1]]
```

Entonces

```
In[27]:= NIF[24106337]
Out[27]= Z
```

### 1.14.4. Definición de funciones de forma recursiva

A continuación vemos diversos ejemplos de funciones definidas recursivamente.

- La función `factorial[n]`:

  ```
  In[28]:= factorial[0]:=1;
  factorial[n_]:=n * factorial[n-1];

  In[30]:= factorial[3]
  Out[30]= 6

  In[31]:= factorial[5]
  Out[31]= 120
  ```

  Para números negativos la función no está bien definida:

```
In[32]:= factorial[-1]
Out[32]= -335085068493297911765266512375481494202258406359174070257677988428620\
879903573277100562613812676331425928080211850228244592655013552225185 6\
727692533193070412811083330325659322041700029792166250734253390513754 4\
660457112403384627010340202629925813784231472766366436471553963053525 4\
110554143943484010991506828543067506859163858198060416294038335658673 9\
198268782104924614076605793562865241982176207428620969776803149467431 3\
868079724382476891586560000000000000000000000000000000000000000000000\
0000000000000000
Hold[factorial[-255-1]]
```

Para que la respuesta sea mas clara podemos definir:

```
In[33]:= f[0]:=1
f[n_Integer]:=n*f[n-1]/;n>0
f[_]:=Print["No se hacerlo"]


In[36]:= f[4]
Out[36]= 24

In[37]:= f[-1]
No se hacerlo
```

- La función `producto[a1,... ,an]` que devuelve el producto $\prod_{i=1}^{n} a_i$:

```
In[38]:= producto[{a1_}]:=a1
         producto[{a1_,a2__}]:=a1*producto[{a2}]

In[40]:= producto[{4,5,6}]
Out[40]= 120

In[41]:= producto[{3,-3,7}]
Out[41]= -63
```

- La función `suma[a1, ... ,an]` que devuelve la suma $\sum_{i=1}^{n} a_i$:

```
In[42]:= suma[{a1_}]:=a1
suma[{a1_,a2__}]:=a1+suma[{a2}]

In[44]:= suma[{1,3,5,9}]
Out[44]= 18

In[45]:= suma[{1,-3,-5}]
Out[45]= -7
```

- Definamos recursivamente la función `mcd[a,b]` (Algoritmo de Euclides):

```
In[46]:= mcd[a_,0]:=a /; a>0
mcd[a_,0]:=-a/;a<0
mcd[a_,b_]:=mcd[b,NResto[a,b]]

In[49]:= mcd[-8,3]
Out[49]= 1

In[50]:= mcd[-12,-10]
Out[50]= 2

In[51]:= mcd[9,-3]
Out[51]= 3
```

- La función `Bezout[a,b]` para calcular el `mcd[a,b]` y enteros $u$ y $v$ (coeficientes de Bezout) tales que `mcd[a,b]=ua+vb`

  Vamos a definir esta función utilizando la función auxiliar `extendidomcd[a_,b_,u0_,u1_,v0_,v1_]` que definimos así:

```
In[52]:= extendidomcd[a_,0,u0_,u1_,v0_,v1_]:={a,{u0,v0}}
extendidomcd[a_,b_,u0_,u1_,v0_,v1_]:=
extendidomcd[b,NResto[a,b],u1,u0-u1*Quotient[a,b],v1,
v0-v1*Quotient[a,b]]
```

  Entonces definimos

```
In[54]:= Bezout[a_,b_]:=extendidomcd[a,b,1,0,0,1]

In[55]:= Bezout[105,389]
Out[55]= {1,{-163,44}}

In[56]:= Bezout[6798765434556,8765487086]
Out[56]= {2,{728111315,-564744205583}}
```

- Usando la función `extendidomcd` para definir la función `emcd[a,b]` que devuelve el máximo común divisor de $a$ y $b$:

  Basta con quedarse con el primer elemento de la lista que la función devuelve

```
In[57]:= emcd[a_,b_]:=extendidomcd[a,b,1,0,0,1][[1]]

In[58]:= emcd[12,36]
Out[58]= 12

In[59]:= emcd[-105,384]
Out[59]= 3
```

- La función `mcdlista[Subscript[a, 1],Subscript[a, 2],...,Subscript[a, n]]` que devuelve el máximo común divisor de la lista `{Subscript[a, 1],Subscript[a, 2],...,Subscript[a, n]}`

```
In[60]:= mcdlista[{a1_,a2_}]:=emcd[a1,a2]
         mcdlista[{a1_,a2_,a3__}]:=emcd[emcd[a1,a2],mcdlista[{a3}]]

In[62]:= mcdlista[{50,8,32,68}]
Out[62]= 2
```

- La función `Diof[a,b,c]` que devuelve una solución de la ecuación diofántica $ax + by = c$

```
In[63]:= Diof[a_,b_,c_]:=If[NResto[c,emcd[a,b]]==0,Quotient[c,emcd[a,b]]*\
         Bezout[a,b][[2]], Print["No tiene solucion"]]

In[64]:= Diof[60,36,12]
Out[64]= {-1,2}

In[65]:= Diof[35,6,8]
Out[65]= {-8,48}

In[66]:= Diof[12,18,11]
No tiene solucion
```

Notemos que, alternativamente, dicha función puede ser definida eludiendo el uso del condicional ïf". Así, podemos definir

```
In[67]:= Dioph[a_,b_,c_]:=Quotient[c,emcd[a,b]]*Bezout[a,b][[2]]/;NResto[c,\
emcd[a,b]]==0
Dioph[_,_,_]:=Print["No tiene solucion"]
```

donde hemos tenido en cuenta:

1. `/;` se lee como "siempre que"
2. Al no necesitar nombres las variables en la segunda línea, usamos simplemente el subrayado (recuérdese que "_" significa "cualquier cosa", y así "a_" significa "cualquier cosa a la que llamamos a").

Entonces

```
In[69]:= Dioph[60,36,12]
Out[69]= {-1,2}

In[70]:= Dioph[35,6,8]
Out[70]= {-8,48}
```

### 1.14.5. Resolución de congruencias y sistemas de congruencias

**La congruencia** $ax \equiv b \pmod{n}$

Recordamos que la congruencia anterior tiene solución si y solo si $d = \text{m.c.d.}(a, n)$ divide a $b$. En este caso, si escribimos $d = ua + vn$ y $b = db'$, sabemos que una solución de la congruencia es $x = ub'$. Definimos una función `CB[a,b,n]` que devuelve una solución de la congruencia $ax \equiv b \pmod{n}$.

```
In[71]:= CB[a_,b_,n_]:=If[Mod[b,GCD[a,n]]==0, \
b/GCD[a,n]*ExtendedGCD[a,n][[2,1]],Print["No tiene solucion"]]
```

Así, una solución de $x \equiv 2 \pmod 3$ la encontramos tomando

```
In[72]:= CB[1,2,3]
Out[72]= 2
```

mientras que la congruencia $2x \equiv 1 \pmod 4$

```
In[73]:= CB[2,1,4]
 No tiene solucion
```

Ejercicio: Dar una definición alternativa de esta función eludiendo el uso del condicional `if` (ver ejemplo anterior con la funcion `Diof` ).

**Sistemas de congruencias**

Recordamos que el sistema

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

tiene solución si y solo si $a_1 \equiv a_2 \pmod{\text{m.c.d.}(n_1, n_2)}$, en cuyo caso, para obtener una solución resolvemos primero la ecuación $n_1 t \equiv a_2 - a_1 \pmod{n_2}$. Si $t_0$ es una solución de esta ecuación, entonces una solución del sistema estará dada por $x_0 = a_1 + t_0 n_1$

Definimos una función `SdosC[{a1, a2]},{n1,n2}]` que encuentre una solución del anterior sistema de congruencias:

```
In[74]:= SdosC[{a1_,a2_},{n1_,n2_}]:=If[Mod[a1-a2,GCD[n1,n2]]==0,a1+CB[n1,a2-\
a1,n2]*n1,Print["No tiene solucion"]]
```

Así, una solución del sistema

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 1 \pmod 6 \end{aligned}$$

la encontramos poniendo

```
In[75]:= SdosC[{3,1},{4,6}]
Out[75]= 7
```

mientras que el sistema

$$\begin{aligned} x &\equiv 5 \pmod 4 \\ x &\equiv 2 \pmod 6 \end{aligned}$$

```
In[76]:= SdosC[{5,2},{4,6}]
 No tiene solucion
```

Esta función nos permite definir a continuación, por recurrencia, una función que devuelve la solución de un sistema general de congruencias. Definimos una función `SCong[{a1,... , ar]},{n1, ... ,nr]}]` que devuelva una solución del sistema

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\dots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

```
In[77]:= SCong[{a1_,a2_},{n1_,n2_}]:=SdosC[{a1,a2},{n1,n2}]
SCong[{a1_,a2_,a3__},{n1_,n2_,n3__}]:=SCong[{SdosC[{a1,a2},{n1,n2}],\
a3},{LCM[n1,n2],n3}]
```

Así, una solución del sistema

$$\begin{aligned} x &\equiv 5 \pmod{11} \\ x &\equiv 6 \pmod{14} \\ x &\equiv 4 \pmod{15} \end{aligned}$$

la encontramos poniendo

```
In[79]:= SCong[{5,6,4},{11,14,15}]
Out[79]= 33214
```

Mientras que la del sistema

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 5 \pmod{7} \\ x &\equiv 5 \pmod{25} \end{aligned}$$

```
In[80]:= SCong[{1,2,5,5},{2,3,7,25}]
Out[80]= 5255
```

Se propone como ejercicio final encontrar solución a los ejercicios propuestos en la sección 1.12 que puedan ser resueltos utilizando las funciones definidas en esta Práctica.

# Capítulo 2

# Anillos conmutativos

## 2.1. Leyes de composición. Estructuras algebraicas.

Sean $A, M$ conjuntos.

**Definición 2.1.1.** Una *operación binaria* o *ley de composición interna* en $A$ es una aplicación

$$A \times A \to A \qquad (a, b) \mapsto a * b$$

Una *acción por la izquierda* o *ley de composición externa* de $A$ sobre $M$ es una aplicación

$$A \times M \to M \qquad (a, x) \mapsto a * x$$

De manera análoga se define una *acción por la derecha* como una aplicación

$$M \times A \to M \qquad (x, a) \mapsto x * a$$

Es costumbre escribir las leyes de composición como operadores "infijo", es decir, con un símbolo entre los elementos. Se suelen usar los símbolos $+, -, *, \cdot, \times, \div, \circ, \diamond$, etc. O bien simplemente yuxtaponiendo los elementos combinados como $ab$ o $ax$.

*Ejemplo* 2.1.2. La suma $a + b$ y el producto $ab$ de números enteros son leyes de composición internas de $\mathbb{Z}$. También existen estas operaciones para los racionales $\mathbb{Q}$, los reales $\mathbb{R}$ y los complejos $\mathbb{C}$.

*Ejemplo* 2.1.3. Sea $n > 0$ un entero fijo y sea $\mathbb{Z}_n$ el conjunto de clases módulo $n$. Hemos definido las operaciones binarias suma y producto como $[a]_n + [b]_n = [a + b]_n$ y $[a]_n[b]_n = [ab]_n$.

En este caso también tenemos una acción $\mathbb{Z} \times \mathbb{Z}_n \to \mathbb{Z}_n$ definida por $a[x]_n = [ax]_n$.

*Ejemplo* 2.1.4. Sea $X$ un conjunto y sea $A = \{f : X \to X\}$ el conjunto de todas las aplicaciones de $X$ en sí mismo. Podemos definir una operación $A \times A \to A$ por $(f, g) \mapsto fg$ donde $fg : X \to X$ viene dada por composición de aplicaciones, es decir que para todo $x \in X$ se define $(fg)(x) = f(g(x))$.

*Ejemplo* 2.1.5. Para cualquier $K$-espacio vectorial $V$ la multiplicación de un escalar por un vector define una acción $K \times V \to V$

*Ejemplo* 2.1.6. Sea $M = M_n(\mathbb{R})$ el conjunto de todas las matrices cuadradas de orden $n$ con coeficientes reales. En $M$ hay definidas dos operaciones internas, la suma y el producto, y una operación externa, el producto de un escalar por una matriz.

*Ejemplo* 2.1.7. Dada una ley de composición $a * b$, se define la *ley de composición opuesta* como $a *^o b = b * a$ para todo $a, b$. Si la ley de partida es interna $A \times A \to A$, también lo es la opuesta. Si la ley es una acción por la izquierda, la opuesta es una acción por la derecha y viceversa.

Una *estructura algebraica* se define por datos de tres tipos:

- Un conjunto $A$, que se llama *conjunto subyacente*.
- Una o varias leyes de composición (internas o externas) definidas sobre $A$.
- Unos axiomas que deben verificar dichas leyes.

En rigor la estructura algebraica está formada por el conjunto $A$ *junto con las operaciones*. Pero por abuso de lenguaje, se suele designar con la misma letra a la estructura y al conjunto subyacente.

Existen muchas estructuras algebraicas, pero las mas importantes son las tres siguientes:

**Definición 2.1.8.** Un *grupo* $(G, *)$ es un conjunto $G$ junto con una ley de composición interna $G \times G \to G$ denotada por $(a, b) \mapsto a * b$ que verifica:

- *Asociatividad:* $\forall\, a, b, c \in G\ a * (b * c) = (a * b) * c$
- *Existencia de neutro:* $\exists\, e \in G\ \forall\, a \in G\ e * a = a = a * e$
- *Existencia de opuesto:* $\forall\, a \in G\ \exists\, a' \in G\ a * a' = e = a' * a$

El elemento $e$ se llama *elemento neutro* para la operación y el elemento $a'$ se llama *opuesto de* $a$.

En el caso particular en que la operación se denote por $a + b$, el elemento neutro se llama *elemento nulo o cero* y se denota por $0$. El opuesto de $a$ se denota por $-a$

Si la operación se denota por $ab$, $a \cdot b$ o $a \times b$, el elemento neutro se llama *unidad o uno* y se denota por $1$. Y el opuesto de $a$ se llama *inverso* y se denota por $a^{-1}$.

Un grupo se llama *conmutativo o abeliano* si verifica el axioma adicional

- *Conmutatividad:* $\forall\, a, b \in G\ a * b = b * a$.

**Definición 2.1.9.** Un *anillo* $(A, +, \cdot)$ es un conjunto $A$ junto con dos operaciones binarias $A \times A \to A$ denotadas por suma $a + b$ y producto $ab$ que verifican los axiomas:

- *Asociatividad de la suma:* $\forall\, a, b, c \in A\ a + (b + c) = (a + b) + c$
- *Existencia de cero:* $\exists\, 0 \in A\ \forall\, a \in A\ 0 + a = a = a + 0$
- *Existencia de opuesto:* $\forall\, a \in A\ \exists\ -a \in A\ a + (-a) = 0 = (-a) + a$
- *Conmutatividad de la suma:* $\forall\, a, b \in A\ a + b = b + a$.

  Estos cuatro primeros axiomas se resumen en uno: $(A, +)$ *es un grupo abeliano*.
- *Asociatividad del producto:* $\forall\, a, b, c \in A\ a(bc) = (ab)c$
- *Distributividad:* $\forall\, a, b, c \in A\ a(b + c) = ab + ac,\ (b + c)a = ba + ca$
- *Existencia de uno:* $\exists\, 1 \in A\ \forall\, a \in A\ 1a = a = a1$

Un anillo se llama *conmutativo o abeliano* si verifica el axioma

- *Conmutatividad del producto:* $\forall\, a, b \in A\ ab = ba$.

Un *anillo de división* es un anillo que verifica el axioma adicional

- *Existencia de inverso:* $\forall\, a \in A,\ a \neq 0,\ \exists\, a^{-1} \in A\ aa^{-1} = 1 = a^{-1}a$

Un *cuerpo* es un anillo de división conmutativo.

**Definición 2.1.10.** Sea $A$ un anillo. Un *módulo por la izquierda sobre* $A$ o *$A$-módulo* $(M, +, \cdot)$ es un conjunto $M$ junto con una ley de composición interna $M \times M \to M$ dada por $(x, y) \mapsto x + y$ y una ley de composición externa $A \times M \to M$ denotada $(a, x) \mapsto ax$ que verifican los axiomas:

- *Asociatividad:* $\forall\, x, y, z \in M\ x + (y + z) = (x + y) + z$
- *Existencia de cero:* $\exists\, 0 \in M\ \forall\, x \in M\ 0 + x = x = x + 0$
- *Existencia de opuesto:* $\forall\, x \in M\ \exists\ -x \in M\ x + (-x) = 0 = (-x) + x$
- *Conmutatividad:* $\forall\, x, y \in M\ x + y = y + x$.
  Estos cuatro primeros axiomas pueden resumirse en uno: $(M, +)$ *es un grupo abeliano*.
- *Distributividad respecto a escalares:* $\forall\, a, b \in A\ \forall\, x \in M\ (a + b)x = ax + bx$
- *Distributividad respecto a vectores:* $\forall\, a \in A\ \forall\, x, y \in M\ a(x + y) = ax + ay$
- *Pseudoasociatividad:* $\forall\, a, b \in A\ \forall\, x \in M\ a(bx) = (ab)x$
- *Acción trivial del uno:* $\forall\, x \in M\ 1x = x$

Los elementos de $M$ se llaman *vectores* y los elementos de $A$ se llaman *escalares*.
En el caso particular en que $A$ es un cuerpo, $M$ se llama *espacio vectorial sobre* $A$.
De manera análoga se define el concepto de *módulo por la derecha sobre* $A$.

**Definición 2.1.11.** Sea $K$ un anillo conmutativo. Un *álgebra (lineal, asociativa y unitaria) sobre* $K$ o una *$K$-álgebra* es un conjunto $A$ junto con dos leyes de composición internas $A \times A \to A$ denotadas por $a + b$ y $ab$ y una ley de composición externa $K \times A \to A$ denotada por $\lambda * a$ que verifican:

- *Asociatividad:* $\forall\, x, y, z \in M\ x + (y + z) = (x + y) + z$
- *Existencia de cero:* $\exists\, 0 \in M\ \forall\, x \in M\ 0 + x = x = x + 0$
- *Existencia de opuesto:* $\forall\, x \in M\ \exists\ -x \in M\ x + (-x) = 0 = (-x) + x$
- *Conmutatividad:* $\forall\, x, y \in M\ x + y = y + x$.
  Estos cuatro primeros axiomas pueden resumirse en uno: $(M, +)$ *es un grupo abeliano*.
- *Distributividad respecto a escalares:* $\forall\, a, b \in A\ \forall\, x \in M\ (a + b)x = ax + bx$
- *Distributividad respecto a vectores:* $\forall\, a \in A\ \forall\, x, y \in M\ a(x + y) = ax + ay$
- *Pseudoasociatividad:* $\forall\, a, b \in A\ \forall\, x \in M\ a(bx) = (ab)x$
- *Acción trivial del uno:* $\forall\, x \in M\ 1x = x$
  Estos ocho axiomas se resumen en uno: $(A, +, *)$ *es un $A$-módulo*.

- *Distributividad:* $\forall\ a, b, c \in A\ a(b + c) = ab + ac,\ (b + c)a = ba + ca$
- *Pseudoasociatividad:* $\forall\ \lambda \in K\ \forall\ a, b \in A\ (\lambda * a)b = \lambda * (ab) = a(\lambda * b)$

  Una $A$-álgebra se llama *asociativa* si verifica el axioma adicional:
- *Asociatividad del producto:* $\forall\ a, b, c \in A\ a(bc) = (ab)c$

  Una $K$-álgebra se llama *unitaria* si verifica el axioma adicional:
- *Existencia de uno:* $\exists\ 1 \in A\ \forall\ a \in A\ 1a = a = a1$
- $(A, +, \cdot)$ es un anillo.

El tipo mas importante de álgebra se puede resumir en tres axiomas:
Sea $K$ un anillo conmutativo. Un *álgebra (lineal, asociativa y unitaria) sobre* $K$ es un conjunto $A$ junto con dos leyes de composición internas $A \times A \to A$ denotadas por $a + b$ y $ab$ y una ley de composición externa $K \times A \to A$ denotada por $\lambda * a$ que verifican:

- $(A, +, *)$ es un $K$-módulo.
- $(A, +, \cdot)$ es un anillo.
- *Pseudoasociatividad:* $\forall\ a, b \in A\ \forall\ x \in M\ a(bx) = (ab)x$

## 2.2. Ejemplos

El que una estructura algebraica resulte interesante depende del número e importancia de los ejemplos que posea. Veamos ejemplos de las estructuras que hemos definido:

### 2.2.1. Ejemplos de grupos

*Ejemplo* 2.2.1. Sea $G = \{e\}$ un conjunto con un único elemento. Sólo hay una operación binaria posible, $e * e = e$. Este grupo $(G, *)$ es el mas pequeño posible y se llama *grupo trivial*. Cualquier grupo con mas de un elemento es un *grupo no trivial*.

*Ejemplo* 2.2.2. Para cualquier grupo $(G, *)$, el *grupo opuesto* $G^o$ es el grupo $(G, *^o)$ donde $*^o$ es la operación opuesta de $*$. En particular, $G$ es abeliano si y sólo si $G = G^o$.

*Ejemplo* 2.2.3. Los ejemplos mas sencillos de grupos son los numéricos. Los casos mas evidentes son:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son grupos para $+$, siendo $0$ el elemento neutro y $-a$ el opuesto de cada $a$.
2. $\mathbb{Q}^\times = \{a \in \mathbb{Q} \mid a \neq 0\}$, $\mathbb{R}^\times = \{a \in \mathbb{R} \mid a \neq 0\}$, $\mathbb{C}^\times = \{a \in \mathbb{C} \mid a \neq 0\}$, $\mathbb{Q}^+ = \{a \in \mathbb{Q} \mid a > 0\}$ y $\mathbb{R}^+ = \{a \in \mathbb{R} \mid a > 0\}$ son grupos para $\times$ con $1$ como elemento neutro y siendo el opuesto de $a$ su inverso $a^{-1} = 1/a$. (Nótese que $\{a \in \mathbb{Z} \mid a \neq 0\}$ *no es un grupo* para $\times$, ya que no todo elemento tiene inverso).
3. Generalizamos el ejemplo anterior: Sea $A$ un anillo arbitrario y sea $A^\times = U(A)$ el conjunto de elementos $a \in A$ que tienen un inverso $a^{-1} \in A$. Entonces $(A, +)$ es un grupo (el *grupo aditivo de* $A$), y $(A^\times, \times)$ también es un grupo (el *grupo multiplicativo de* $A$), .
4. Los axiomas para un espacio vectorial $V$ sobre un cuerpo $K$ incluyen en particular el hecho de que $(V, +)$ es un grupo abeliano. En particular, $\mathbb{R}^n$ es un grupo aditivo.

5. Para todo número $n \in \mathbb{Z}$, $n > 0$, $\mathbb{Z}/n\mathbb{Z}$ es un anillo, así que $(\mathbb{Z}/n\mathbb{Z}, +)$ y $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ son grupos, donde $(\mathbb{Z}/n\mathbb{Z})^\times = U(\mathbb{Z}/n\mathbb{Z}) = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (\text{m. c. d.})(a, n) = 1\}$.

No deben confundirse los grupos $\mathbb{Z}/n\mathbb{Z}$ (bajo la suma) y $(\mathbb{Z}/n\mathbb{Z})^\times$ (bajo multiplicación), aunque el último sea un subconjunto del primero, *no es un subgrupo*.

### 2.2.2. Ejemplos de anillos

*Ejemplo* 2.2.4. Sea $A = \{a\}$ un conjunto con un único elemento. En este caso sólo hay una operación binaria posible, y por tanto la suma y el producto coinciden: $a + a = a = aa$ y $0 = a = 1$. Este anillo $(A, +, \cdot)$ es el mas pequeño posible y se llama *anillo trivial*. Cualquier anillo con mas de un elemento es un *anillo no trivial*.

*Ejemplo* 2.2.5. Para cualquier anillo $(A, +, \cdot)$, definimos el *anillo opuesto* $A^o$ como el anillo $(A, +, \cdot^o)$ donde $\cdot^o$ es la operación opuesta de $\cdot$; en particular, $A$ es abeliano si y sólo si $A = A^o$.

*Ejemplo* 2.2.6. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son anillos conmutativos respecto a la suma y producto usuales. En todos los casos el neutro para la suma es el númerol 0 y el neutro para el producto es el número 1. Además $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son cuerpos.

*Ejemplo* 2.2.7. Para todo natural positivo $n$ las clases de restos módulo $n$, $\mathbb{Z}_n$ con la suma y producto de clases es también un anillo conmutativo. Este anillo es un cuerpo si y sólo si $n$ es primo.

*Ejemplo* 2.2.8. Sea $\mathbb{J} = \{a + bi \mid a, b \in \mathbb{Z},\ i^2 = -1\} \subset \mathbb{C}$. Para cualesquiera $a + bi, c + di \in \mathbb{J}$ se verifica

$$\begin{aligned} (a + bi) + (c + di) &= (a + c) + (b + d)i \in \mathbb{J}, \\ (a + bi)(c + di) &= (ac - bd) + (ad + bc)i \in \mathbb{J}, \\ 0, 1 &\in \mathbb{J}, \\ -(a + bi) &= (-a) + (-b)i \in \mathbb{J}. \end{aligned}$$

Como la suma y el producto de números complejos son asociativas y conmutativas y verifican la distributividad, tenemos un anillo conmutativo $(\mathbb{J}, +, \cdot)$ que se llama *anillo de los enteros de Gauss*.

*Ejemplo* 2.2.9. Sea $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$. Es obvio que este conjunto es cerrado para la suma y el producto, y como estas operaciones son asociativas y conmutativas en $\mathbb{R}$, también lo son en $\mathbb{Q}(\sqrt{2})$. De la misma manera se comprueba que el producto es distributivo respecto a la suma. Además $0 = 0 + 0\sqrt{2}$ y $1 = 1 + 0\sqrt{2}$ pertenecen a $\mathbb{Q}(\sqrt{2})$, y para todo $x = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ se verifica que $-x = (-a) + (-b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. En resumen, $\mathbb{Q}(\sqrt{2})$ es un anillo.

Para ver que es un cuerpo, observamos que para todo $a + b\sqrt{2} \in \mathbb{Q}$ distinto de cero se verifica que $a^2 - 2b^2 \neq 0$ (porque en otro caso, $\sqrt{2}$ sería racional). Así que

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

luego es un cuerpo.

*Ejemplo* 2.2.10. Un subconjunto interesante del ejemplo anterior es

$$\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$$

que obviamente es cerrado para la suma, el producto, el cero y el uno. Para un elemento $u = m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ el inverso $u^{-1}$ pertenece a $\mathbb{Z}[\sqrt{2}]$ si y sólo si $m^2 - 2n^2 = \pm 1$.

*Ejemplo* 2.2.11. Un tipo de anillos importantes son los anillos de funciones. Sea $X$ cualquier conjunto no vacío y sea $A$ un anillo arbitrario. Sea $B = \{f : X \to A\}$. Definimos en $B$ una suma y un producto punto a punto: $(f + g)(x) = f(x) + g(x)$ y $(fg)(x) = f(x)g(x)$. De cada axioma de anillo de $A$ se deduce el axioma correspondiente en $B$. El anillo $B$ es conmutativo si y sólo si lo es $A$.

Si $X$ y $A$ tienen mas estructura podemos formar otros anillos de funciones que respetan esta estructura. Por ejemplo si $A = \mathbb{R}$ y $X$ es el intervalo cerrado $X = [0, 1] \subset \mathbb{R}$ podemos formar el anillo conmutativo $B$ de las funciones continuas $[0, 1] \to \mathbb{R}$. Los teoremas básicos sobre límites nos garantizan que la suma y el producto de funciones continuas son también funciones continuas.

*Ejemplo* 2.2.12. Sea $A$ un anillo arbitrario y sea $n > 0$ un entero. Sea $M_n(A)$ el conjunto de todas las matrices $n \times n$ con coeficientes en $A$. Este conjunto es un anillo para las operaciones usuales de suma y producto de matrices. Si $n > 1$, el anillo $M_n(A)$ no es conmutativo

*Ejemplo* 2.2.13. Sea $A$ un anillo conmutativo. El conjunto $A[X]$ de todos los polinomios en una indeterminada con coeficientes en $A$ junto con la suma y el producto es un anillo conmutativo.

### 2.2.3. Ejemplos de módulos

*Ejemplo* 2.2.14. El grupo abeliano $\mathbb{Z}_n$ es un $\mathbb{Z}$-módulo con la acción

$$\mathbb{Z} \times \mathbb{Z}_n \to \mathbb{Z}_n$$

definida por $a[b]_n = [ab]_n$.

*Ejemplo* 2.2.15. Todo grupo abeliano $M$ es un $Z$-módulo de manera única, definiendo la acción $\mathbb{Z} \times M \to M$ por inducción:

$$ax = \begin{cases} 0 & \text{si } a = 0 \\ (a-1)x + x & \text{si } a > 0 \\ -(-ax) & \text{si } a < 0 \end{cases}$$

*Ejemplo* 2.2.16. El conjunto de vectores libres (del plano o del espacio) con la suma por la "regla del paralelogramo" y el producto escalar usual forman un espacio vectorial sobre $\mathbb{R}$ (De hecho la nomenclatura y las propiedades intuitivas provienen de este ejemplo).

*Ejemplo* 2.2.17. Sean $K$ un cuerpo, $M$ un espacio vectorial sobre $K$ y $t : M \to M$ una aplicación lineal. Definimos una ley externa $K[X] \times M \to M$ como

$$(a_m X^m + a_{m-1} X^{m-1} + \cdots + a_2 X^2 + a_1 X + a_0) \cdot u = a_m t^m(u) + a_{m-1} t^{m-1}(u) + \cdots + a_2 t^2(u) + a_1 t(u) + a_0 u$$

Con esta operación, $M$ pasa a ser un $K[X]$-módulo (de hecho, todos los $K[X]$-módulos se obtienen de esta manera).

### 2.2.4. Ejemplos de álgebras

*Ejemplo* 2.2.18. Sea $M$ un $A$-módulo arbitrario. Para cualesquiera $x, y \in M$ definimos $xy = 0$. Con este producto obtenemos un álgebra asociativa, aunque no unitaria.

*Ejemplo* 2.2.19. Cualquier anillo $A$ es una $\mathbb{Z}$-álgebra (asociativa y unitaria) de manera única.

*Ejemplo* 2.2.20. Todo anillo conmutativo $A$ es un $A$-álgebra definiendo el producto externo igual al producto interno del anillo.

*Ejemplo* 2.2.21. Los números complejos con las operaciones usuales son un álgebra sobre los reales.

*Ejemplo* 2.2.22. Sea $A$ un anillo *conmutativo*. Las matrices cuadradas $M_n(A)$ con la suma, producto y producto escalar usuales forman un $A$-álgebra (asociativa y unitaria).

*Ejemplo* 2.2.23. Sea $A$ un anillo conmutativo. El conjunto $A[X]$ de todos los polinomios en una indeterminada con coeficientes en $A$ junto con la suma, producto y producto escalar usuales es un álgebra sobre $A$ (asociativa, conmutativa y unitaria).

*Ejemplo* 2.2.24. Sea $K$ un cuerpo y sea $n > 1$. En el conjunto de matrices cuadradas $M_n(K)$ definimos un nuevo producto: $[A, B] = AB - BA$, donde el producto del segundo miembro es el producto usual de matrices (este nuevo producto se llama *corchete de Lie*). El conjunto $M_n(K)$ con la suma, el corchete de Lie y el producto escalar forma un álgebra no asociativa

## 2.3. Reglas de cálculo

De los axiomas de cada estructura algebraica se deducen unas cuantas consecuencias sencillas pero importantes para manipular expresiones y realizar cálculos en la estructura, y por ello se llaman *reglas de cálculo*. Vamos a estudiar las correspondientes a grupos y anillos.

### 2.3.1. Reglas de cálculo para grupos

**Proposición 2.3.1.** *Sea $G$ un grupo con unidad $e$.*

1. *La unidad de un grupo es única*
2. *El inverso de cualquier elemento es único*
3. *(*Propiedad cancelativa*): Para $x, y, z \in G$,*
$$xy = xz \Rightarrow y = z \qquad yx = zx \Rightarrow y = z$$
4. $e^{-1} = e$
5. *Para todo elemento $x \in G$ se verifica $(x^{-1})^{-1} = x$*
6. *Para cualesquiera $x, y \in G$ se verifica $(xy)^{-1} = y^{-1}x^{-1}$*
7. *Para cualesquiera $x, y \in G$ existen únicos $u, v \in G$ tales que $xu = y$ y $vx = y$.*

*Demostración.* 1. Sean $e, f \in G$ dos unidades. Entonces $e = ef = f$

2. Sean $x', x^{-1}$ dos inversos para $x \in G$. Entonces $x' = x'e = x'(xx^{-1}) = (x'x)x^{-1} = ex^{-1} = x^{-1}$
3. Sea $xy = xz$. Multiplicamos ambos miembros por $x^{-1}$ por la izquierda: $y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z$. Igual por el otro lado.
4. De la misma definición: $ee = e$, luego $e = e^{-1}$
5. Por definición, $xx^{-1} = e = x^{-1}x$, luego de la misma definición de inverso obtenemos que $(x^{-1})^{-1} = x$
6. Un simple cálculo: $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = e$, luego $(xy)^{-1} = y^{-1}x^{-1}$
7. Otro simple cálculo muestra que $u = x^{-1}y$ y $v = yx^{-1}$ verifican las condiciones pedidas y son los únicos que las verifican.

□

Las propiedad asociativa garantiza que en un cálculo podemos introducir paréntesis arbitrariamente: Sean $x_1, \dots x_n \in G$. Definimos por recurrencia: $\prod_{i=1}^{n} x_i = (\prod_{i=1}^{n-1} x_i)x_n$.

**Proposición 2.3.2** (Ley asociativa general)**.** *Sea $G$ un conjunto con una operación interna asociativa. Para cualesquiera enteros $m > n > 0$ sean $x_1, \dots x_m$ elementos de $G$. Se verifica*

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

*Demostración.* Por inducción sobre $m - n$ (el número de factores del segundo producto). Si $m - n = 1$, la expresión dada es

$$\left(\prod_{i=1}^{n} x_i\right) x_{n+1} = \prod_{i=1}^{n+1} x_i$$

Sea ahora $m - n = k > 1$ y suponemos cierto el resultado cierto siempre que el segundo producto del primer miembro tenga menos de $k$ factores. Calculamos usando la propiedad asociativa:

$$\left(\prod_{i=1}^{n} x_i\right)\left(\prod_{i=n+1}^{m} x_i\right) = \left(\prod_{i=1}^{n} x_i\right)\left(\left(\prod_{i=n+1}^{m-1} x_i\right) x_m\right) =$$

$$\left(\left(\prod_{i=1}^{n} x_i\right)\left(\prod_{i=n+1}^{m-1} x_i\right)\right) x_m = \left(\prod_{i=1}^{m-1} x_i\right) x_m = \prod_{i=1}^{m} x_i$$

□

De la misma forma, cuando se verifica la propiedad conmutativa podemos multiplicar los elementos en cualquier orden:

**Proposición 2.3.3** (Ley conmutativa general)**.** *Sea $G$ un conjunto con una operación interna que es asociativa y conmutativa. Sean $x_1, \dots, x_n \in G$ y sea $\sigma$ una permutación del conjunto $\{1, \dots, n\}$. Se verifica:*

$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{n} x_{\sigma(i)}$$

*Demostración.* Por inducción sobre $n$. Para $n = 2$ sólo hay dos permutaciones: La identidad $\sigma_0$ y la trasposición $\sigma_1 = (1\ 2)$. Para $\sigma_0$ la igualdad es trivial: $x_1x_2 = x_1x_2$. Y para $\sigma_1$ es el enunciado de la propiedad conmutativa: $x_1x_2 = x_2x_1$.

Sea ahora $n > 2$ y suponemos el resultado cierto para todo producto con menos factores. Sea $k = \sigma(n)$. Entonces para todo $i \neq k$ existe un $j < n$ tal que $i = \sigma(j)$.

Calculamos:

$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{k-1} x_i \left(x_k \prod_{i=k+1}^{n} x_i\right) = \prod_{i=1}^{k-1} x_i \left(\left(\prod_{i=k+1}^{n} x_i\right) x_k\right) =$$

$$\left(\prod_{i=1}^{k-1} x_i \left(\prod_{i=k+1}^{n} x_i\right)\right) x_k = \left(\prod_{j=1}^{n-1} x_{\sigma(j)}\right) x_{\sigma(n)} = \prod_{i=1}^{n} x_{\sigma(i)}$$

□

Sea $(G, \cdot)$ un grupo con elemento neutro 1 y sea $a \in G$ arbitrario. Para todo entero positivo $n$ definimos por inducción: $a^0 = 1$ y $a^n = (a^{n-1})a$. Para $n < 0$ definimos también $a^n = (a^{-1})^{-n}$.

Si la operación se denota aditivamente, la notación que se usa es $na$.

**Proposición 2.3.4.** *Para todo $a \in G$ y cualesquiera $m, n \in \mathbb{Z}$ se verifica:*

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

*Si $a, b \in G$ y $ab = ba$, entonces para todo $n \in \mathbb{Z}$ se verifica*

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

*Demostración.* Todos los casos se demuestran por inducción sobre $n$. □

Si el grupo se denota aditivamente, las expresiones de la proposición anterior son

$$(m + n)a = ma + na, \qquad (nm)a = n(ma), \qquad n(a + b) = na + nb$$

**Corolario 2.3.5.** *Todo grupo abeliano es un $\mathbb{Z}$-módulo de manera única*

Este corolario nos dice que los conceptos "$\mathbb{Z}$-módulo" y "grupo abeliano" son idénticos.

Si $m > n$ y $a^m = a^n$, necesariamente $a^{m-n} = 1$. Luego si en algún momento la sucesión $a^0, a^1, a^2, \ldots$ se repite, necesariamente el primer término que se repite es $a^0 = 1$.

**Definición 2.3.6.** Sea $G$ un grupo y sea $a \in G$. Si para todo $n > 0$ se verifica $a^n \neq 1$, decimos que el orden de $a$ es infinito y lo representamos por $o(a) = \infty$.

En otro caso, el menor $k > 0$ que verifica $a^k = 1$ se llama orden de $a$ y se representa por $o(a) = k$. En este caso decimos que $a$ es un *elemento de orden finito* o que es un *elemento de torsión*.

### 2.3.2. Reglas de cálculo para anillos

**Proposición 2.3.7.** *Sea $A$ un anillo.*

1. *Para todo $a \in A$ se verifica $a0 = 0 = 0a$*
2. *Si $A$ no es el anillo trivial, $0 \neq 1$.*
3. *Para todo $a, b \in A$, $(-a)b = -(ab) = a(-b)$. En particular $-a = (-1)a$.*
4. *Para todo $a, b \in A$, $(-a)(-b) = ab$. En particular $(-1)(-1) = 1$.*

*Demostración.*

1. $a + 0 = a$. Multiplicamos por $a$ y usamos la propiedad distributiva: $aa + a0 = a(a + 0) = aa$. Restamos $aa$ y obtenemos $a0 = 0$. Igual por el otro lado.
2. Si $0 = 1$, para todo $a \in A$ se verifica $a = a1 = a0 = 0$ y $A$ es el anillo trivial.
3. Por la primera regla y la distributividad,

$$0 = 0b = (a + (-a))b = ab + (-a)b$$

Restando $ab$ de ambos miembros obtenemos $-(ab) = (-a)b$. Igual por el otro lado.

4. Corolario inmediato de la regla anterior.

□

**Proposición 2.3.8** (Ley distributiva general). *Sea $A$ un anillo. Para cualesquiera $a_1, \dots, a_n, b_1, \dots, b_m \in A$ se verifica*

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

*Demostración.* Por doble inducción sobre $m$ y $n$. Para $m = 1$ y $n = 2$ es la propiedad distributiva. Sea $m = 1$ y $n > 2$. Por inducción sobre $n$:

$$\left(\sum_{i=1}^{n} a_i\right) b_1 = \left(\left(\sum_{i=1}^{n-1} a_i\right) + a_n\right) b_1 = \left(\sum_{i=1}^{n-1} a_i\right) b_1 + a_n b_1 =$$

$$\left(\sum_{i=1}^{n-1} a_i b_1\right) + a_n b_1 = \left(\sum_{i=1}^{n} a_i b_1\right)$$

Sea ahora $m > 1$. Por inducción

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

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

$$\sum_{i=1}^{n}\sum_{j=1}^{m-1} a_i b_j + \sum_{i=1}^{n} a_i b_m = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$

□

**Corolario 2.3.9.** *Para todo $n \in \mathbb{Z}$ y todo $a, b \in A$ se verifica*

$$(na)b = n(ab) = a(nb)$$

**Proposición 2.3.10** (Teorema del binomio). *Sea $A$ un anillo conmutativo y sea $n$ un entero positivo. Para todo $a, b \in A$ se verifica*

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

**Definición 2.3.11.** La *característica* de un anillo $A$ es el orden de 1 en el grupo aditivo $(A, +)$ si este orden es finito. En otro caso la característica de $A$ es cero. Se representa por $car(A)$.

Es decir, $car(A) = m > 0$ si $m$ es el menor entero positivo tal que $m \cdot 1 = 0$. Si para todo $n > 0$ se verifica $n \cdot 1 \neq 0$, entonces $car(A) = 0$.

**Proposición 2.3.12.** *Sea $car(A) = m$. Entonces para todo $a \in A$ se verifica $ma = 0$*

*Demostración.* Si $car(A) = 0$ el resultado es trivial. Supongamos $car(A) = m > 0$. Para cualquier $a \in A$ tenemos $ma = m(1a) = (m1)a = 0a = 0$. □

## 2.4. Homomorfismos

### 2.4.1. Homomorfismos de grupos

**Definición 2.4.1.** Dados dos grupos $G$ y $H$ llamamos *homomorfismo* de $G$ a $H$ a toda aplicación $f : G \to H$ tal que para todo par $x, y \in G$ verifique $f(xy) = f(x)f(y)$

*Ejemplo* 2.4.2. La aplicación signo $sgn : S_n \to \{1, -1\}$ es un homomorfismo de grupos.

*Ejemplo* 2.4.3. La aplicación logaritmo $\log : \mathbb{R}^+ \to \mathbb{R}$ es un homomorfismo del grupo multiplicatio $(\mathbb{R}^+, \times)$ en el grupo aditivo $(\mathbb{R}, +)$.

*Ejemplo* 2.4.4. Sea $K$ un cuerpo. Llamamos *grupo lineal general* sobre $K$ y representamos por $GL_n(K)$ al grupo $U(M_n(K))$, es decir al conjunto de todas las matrices $n \times n$ invertibles con la operación producto de matrices. La aplicación determinante $det : GL_n(K) \to K^\times = U(K)$ que asigna a cada matriz su determinante es un homomorfismo de grupos.

Para un homomorfismo $f$ arbitrario el grupo $G$ se llama *dominio* de $f$ y el grupo $H$ se llama *codominio* o *rango* de $f$.

El conjunto $\mathrm{Im}(f) = f(G) = \{f(x) \mid x \in G\} \subset H$ se llama *imagen de* $f$ y el conjunto $\ker(f) = \{x \in G \mid f(x) = 1\} \subset G$ se lama *núcleo de* $f$

Un homomorfismo de grupos $f$ se llama *monomorfismo* si es una aplicación inyectiva, se llama *epimorfismo* si es una aplicación suprayectiva. Se llama *isomorfismo* si es una biyección y se representa por $f : G \cong H$.

Si el dominio y el codominio coinciden, $G = H$, diremos que $f$ es un *endomorfismo*. Un endomorfismo biyectivo se llama *automorfismo*.

**Proposición 2.4.5.** *1. Para todo grupo $G$ la aplicación identidad $1_G : G \to G$ es un automorfismo.*

*2. Sean $f_1 : G \to H$, $f_2 : H \to K$ dos homomorfismos de grupos. Entonces la aplicación compuesta $f_2 f_1 : G \to K$ es un homomorfismo.*

*3. Sea $f : G \to H$ un isomorfismo de grupos. Entonces la aplicación inversa $f^{-1} : H \to G$ también es un isomorfismo.*

**Corolario 2.4.6.** *Para un grupo arbitrario $G$, el conjunto de todos los automorfismos de $G$ forman un grupo (con la composición de aplicaciones como operación), que se llama* grupo de los automorfismos de $G$ *y se representa por* $\mathrm{Aut}(G)$

**Proposición 2.4.7.** *Todo homomorfismo de grupos $f : G \to H$ verifica:*

1. $f(1) = 1$
2. $\forall x \in G\ f(x^{-1}) = f(x)^{-1}$

*Demostración.* 1. $f(1) \cdot 1 = f(1) = f(1 \cdot 1) = f(1)f(1)$. Simplificando nos queda $1 = f(1)$.

2. $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1})$, luego $f(x^{-1}) = f(x)^{-1}$.

□

### 2.4.2. Homomorfismos de anillos

Sean $A$ y $B$ dos anillos.

**Definición 2.4.8.** Un *homomorfismo* de $A$ a $B$ es una aplicación $f : A \to B$ que verifica:

$$\forall x, y \in A \; f(x+y) = f(x) + f(y)$$
$$\forall x, y \in A \; f(xy) = f(x)f(y)$$
$$f(1) = 1$$

Obsérvese que la última condición no se deduce de las dos primeras:

*Ejemplo* 2.4.9. Sea $B$ un anillo no trivial y sea $f$ la aplicación cero. Entonces $f(1) = 0 \neq 1$, aunque $f(x+y) = 0 = f(x) + f(y)$ y $f(xy) = 0 = f(x)f(y)$.

*Ejemplo* 2.4.10. Sea $f : \mathbb{Z} \to \mathbb{Z}_n$ la aplicación definida por $f(x) = [x]_n$. Esta $f$ es un homomorfismo de anillos.

*Ejemplo* 2.4.11. En general, para cualquier anillo $A$ existe un único homomorfismo de anillos $u : \mathbb{Z} \to A$, que viene dado por $u(n) = n \cdot 1$ y que se llama *homomorfismo unital* de $A$.

*Ejemplo* 2.4.12. Sea $A$ un anillo conmutativo y sea $a \in A$ arbitrario. La *evaluación en a* $E_a : A[X] \to A$ definida por $E_a(f(X)) = f(a)$ es un homomorfismo de anillos

Para cualquier homomorfismo $f$ el anillo $A$ se llama *dominio* de $f$ y el anillo $B$ se llama *codominio* o *rango* de $f$.

El conjunto $\mathrm{Im}(f) = f(A) = \{f(x) \mid x \in A\} \subset B$ se llama *imagen de* $f$ y el conjunto $\ker(f) = \{x \in A \mid f(x) = 0\} \subset A$ se llama *núcleo de* $f$

El homomorfismo de anillos $f$ se llama *monomorfismo* si es una aplicación inyectiva, se llama *epimorfismo* si es una aplicación suprayectiva. Se llama *isomorfismo* si es una biyección y se representa por $f : A \cong B$.

Si el dominio y el codominio coinciden, $A = B$, diremos que $f$ es un *endomorfismo*. Un endomorfismo biyectivo se llama *automorfismo*.

**Proposición 2.4.13.** *1. Para todo anillo $A$ la aplicación identidad $1_A : A \to A$ es un automorfismo.*

2. *Sean $f_1 : A \to B$, $f_2 : B \to C$ dos homomorfismos de anillos. Entonces la aplicación compuesta $f_2 f_1 : A \to C$ es un homomorfismo.*

3. *Sea $f : A \to B$ un isomorfismo de anillos. Entonces la aplicación inversa $f^{-1} : B \to A$ también es un isomorfismo*

**Corolario 2.4.14.** *Para un anillo arbitrario $A$, el conjunto de todos los automorfismos de $A$ forman un grupo (con la composición de aplicaciones como operación), que se llama* grupo de los automorfismos de *$A$ y se representa por* $\mathrm{Aut}(A)$

### 2.4.3. Homomorfismos de módulos

Sea $A$ un anillo y sean $M$ y $N$ dos $A$-módulos por la izquierda.

**Definición 2.4.15.** Un *homomorfismo de $A$-módulos* es una aplicación $f : M \to N$ que verifica:

$$\forall x, y \in M \; f(x+y) = f(x) + f(y)$$
$$\forall a \in A \; \forall x \in M \; f(ax) = af(x)$$

El módulo $M$ se llama *dominio* de $f$ y el módulo $N$ se llama *codominio* o *rango* de $f$.

El conjunto $\mathrm{Im}(f) = f(M) = \{f(x) \mid x \in M\} \subset N$ se llama *imagen de* $f$ y el conjunto $\ker(f) = \{x \in M \mid f(x) = 0\} \subset M$ se lama *núcleo de* $f$

El homomorfismo de módulos $f$ se llama *monomorfismo* si es una aplicación inyectiva, se llama *epimorfismo* si es una aplicación suprayectiva. Se llama *isomorfismo* si es una biyección y se representa por $f : M \cong N$.

Si el dominio y el codominio coinciden, $M = N$, diremos que $f$ es un *endomorfismo*. Un endomorfismo biyectivo se llama *automorfismo*.

**Proposición 2.4.16.** *1. Para todo módulo M la aplicación identidad $1_M : M \to M$ es un automorfismo.*

2. *Sean $f_1 : M \to N$, $f_2 : N \to L$ dos homomorfismos de módulos. Entonces la aplicación compuesta $f_2 f_1 : M \to L$ es un homomorfismo.*

3. *Sea $f : M \to N$ un isomorfismo de módulos. Entonces la aplicación inversa $f^{-1} : N \to M$ también es un isomorfismo.*

4. *Sean $f_1, f_2 : M \to N$ y sea $a \in A$ arbitrario dos homomorfismos de módulos. Entonces las aplicaciones $f_1 + f_2, af_1 : M \to L$ son homomorfismos.*

**Corolario 2.4.17.** *Para dos módulos arbitrarios M, N el conjunto de todos los homomorfismos $f : M \to N$ forman un A-módulo (con la suma y el producto por escalares como operaciones) que se representa por* $\mathrm{Hom}_A(M, N)$.

*Para un módulo arbitrario M, el conjunto de todos los endomorfismos de M forman un anillo (con la suma y la composición de aplicaciones como operaciones), que se llama* anillo de los endomorfismos de *M y se representa por* $\mathrm{End}_A(M)$

*Para un módulo arbitrario M, el conjunto de todos los automorfismos de M forman un grupo (con la composición de aplicaciones como operación), que se llama* grupo de los automorfismos de *M y se representa por* $\mathrm{Aut}_A(M)$

## 2.5. Subestructuras

### 2.5.1. Subgrupos

**Definición 2.5.1.** Dados dos grupos $(G, \cdot)$ y $(H, \circ)$, decimos que *H es un subgrupo de G*, y lo representamos por $H < G$, cuando H es un subconjunto de $G$ y la aplicación de inserción $H \to G$ es un homomorfismo de grupos.

*Ejemplo* 2.5.2. Todo grupo $G$ tiene dos subgrupos: El grupo formado sólo por el elemento unidad, que es el *subgrupo trivial*, y el mismo $G$, que es el *subgrupo total*. Ambos son los *subgrupos impropios*. Cualquier otro subgrupo es un *subgrupo propio*.

Por abuso de lenguaje se suele identificar al subgrupo $(H, \circ)$ con el subconjunto $H$, ya que la ley de composición está determinada por el grupo $G$.

**Proposición 2.5.3** (Caracterizaciones de subgrupo)**.** *1. Sea G un grupo y sea $\emptyset \neq H \subset G$. Entonces H es un subgrupo de G si y sólo si se verifica:*

   a) *Para todo par de elementos $x, y \in H$ también $xy \in H$.*
   b) $1 \in H$
   c) *Para todo $x \in H$ también $x^{-1} \in H$.*

2. *Sea G un grupo y sea $\emptyset \neq H \subset G$. Entonces H es un subgrupo de G si y sólo si para todo par de elementos $x, y \in H$ se verifica que $xy^{-1} \in H$.*

3. *Sea G un grupo* finito *y sea $\emptyset \neq H \subset G$. Entonces H es un subgrupo de G si y sólo si para todo par de elementos $x, y \in H$ se verifica que $xy \in H$.*

*Demostración.* 1. Trivial

2. Sea $H$ un subgrupo de $G$ y sean $x, y \in H$. Por ser $H$ un subgrupo es cerrado para el inverso, luego $y^{-1} \in H$, y para la composición, luego $xy^{-1} \in H$.

   Sea ahora $H$ un subconjunto de $G$ no vacío verificando la propiedad del enunciado. Por ser no vacío existe un $x \in H$, luego $1 = xx^{-1} \in H$ y $x^{-1} = 1x^{-1} \in H$. Y para cualesquiera $x, y \in H$, $xy = x(y^{-1})^{-1} \in H$. As¡ que $H$ es cerrado para la unidad, el inverso y la composición. Luego es un subgrupo de $G$.

3. Por ser $G$ un grupo finito, $\forall x \in G\ \exists n > 0\ x^n = 1$ y por tanto $x^{-1} = x^{n-1}$. Por inducción sobre $n$, de la propiedad del enunciado y de $x \in H$ deducimos que $x^{n-1} \in H$. El resto es igual al apartado anterior. □

*Ejemplo* 2.5.4. Para cualquier homomorfismo de grupos $f : G \to H$, el conjunto $\ker(f)$ es un subgrupo de $G$ y el conjunto $\mathrm{Im}(f)$ es un subgrupo de $H$.

**Proposición 2.5.5.** *Sea $K$ subgrupo de $H$ y sea $H$ subgrupo de $G$. Entonces $K$ es un subgrupo de $G$.*

Como ilustración del criterio vamos a demostrar:

**Proposición 2.5.6.** *Sea $\{H_\lambda \mid \lambda \in \Lambda\}$ una familia de subgrupos de un grupo $G$. Entonces $H = \cap_\lambda H_\lambda$ es un subgrupo de $G$.*

*Demostración.* Sea 1 el elemento unidad de $G$ Para todo $\lambda$, $1 \in H_\lambda$ as¡ que $1 \in \cap_\lambda H_\lambda$ y por tanto $H$ es no vacío.

Sean ahora $x, y \in H$ arbitrarios. Para todo $\lambda$ se verifica que $x, y \in H_\lambda$ y por ser $H_\lambda$ un subgrupo tenemos que $\forall \lambda\ xy^{-1} \in H_\lambda$. Luego $xy^{-1} \in \cap H_\lambda = H$. □

Esta proposición nos permite definir dos conceptos importantes:

**Definición 2.5.7.** Sea $S$ un subconjunto de $G$. Llamamos *subgrupo generado por $S$* a la intersección $H$ de todos los subgrupos de $G$ que contienen a $S$. Lo representamos por $H = \langle S \rangle$.

**Definición 2.5.8.** Sea $\{H_\lambda \mid \lambda \in \Lambda\}$ una familia arbitraria de subgrupos de $G$. Llamamos *compuesto de los $H_\lambda$* al subgrupo generado por $S = \cup_\lambda H_\lambda$. Lo representamos por $\vee_\lambda H_\lambda$

En el caso particular en que la familia es finita, sea $H_1, \ldots, H_n$, su compuesto se representa por $H_1 \vee \cdots \vee H_n$.

**Proposición 2.5.9.** *1. Sea $S = \emptyset$. Entonces $\langle S \rangle$ es el subgrupo trivial.*

2. *Para cualquier $S \subset G$ no vacío, $\langle S \rangle$ es el conjunto de todos los elementos de $G$ que se expresan como producto finito de elementos de $S$ y de sus inversos.*

3. *Sea $G$ un grupo finito. Para cualquier $S \subset G$ no vacío, $\langle S \rangle$ es el conjunto de todos los elementos de $G$ que se expresan como producto finito de elementos de $S$.*

### 2.5.2. Subanillos e ideales

**Definición 2.5.10.** Dados dos anillos $(A, +, \cdot)$ y $(B, +, \circ)$, decimos que *$B$ es un subanillo de $A$*, y lo representamos por $B < A$, cuando B es un subconjunto de $A$ y la aplicación de inserción $B \to A$ es un homomorfismo de anillos.

Todo anillo $A$ tiene dos subanillos: El anillo formado por los múltiplos de 1, que es el *subanillo primo*, y el mismo $A$, que es el *subanillo total*. Este último es el *subanillo impropio*. Cualquier otro subanillo es un *subanillo propio*.

Por abuso de lenguaje se suele identificar al subanillo $(B, +, \circ)$ con el subconjunto $B$, ya que la ley de composición está determinada por el anillo $A$.

**Proposición 2.5.11** (Caracterizaciones de subanillo)**.** *1. Sea $A$ un anillo y sea $\emptyset \neq B \subset A$. Entonces $B$ es un subanillo de $A$ si y sólo si se verifica:*

a) *Para todo par de elementos $x, y \in B$ también $x + y, xy \in B$.*

b) $0, 1 \in B$

c) *Para todo $x \in B$ también $-x \in B$.*

*2. Sea $A$ un anillo y sea $\emptyset \neq B \subset A$. Entonces $B$ es un subanillo de $A$ si y sólo si para todo par de elementos $x, y \in B$ se verifica que $x - y, xy \in B$ y además $1 \in B$.*

Obsérvese que para que $B$ sea subanillo de $A$ hay que comprobar explícitamente que la identidad es la misma en $A$ que en $B$.

*Ejemplo* 2.5.12. El anillo $\mathbb{Z}$ es un subanillo de $\mathbb{Z}[i]$ y de $\mathbb{Z}[\sqrt{2}]$. Ninguno de estos dos es un subanillo del otro, aunque ambos son subanillo de $\mathbb{C}$.

Además el anillo $\mathbb{Z}[\sqrt{2}]$ es un subanillo de $\mathbb{Q}(\sqrt{2})$.

*Ejemplo* 2.5.13. El subconjunto $\{[0], [2], [4]\} \subset \mathbb{Z}_6$ es un anillo con unidad $[4]$, pero no es un subanillo de de $\mathbb{Z}_6$ porque el elemento neutro no es el mismo.

*Ejemplo* 2.5.14. Sea $A = M_n(\mathbb{R})$ el anillo de todas las matrices $n \times n$ con coeficientes en $\mathbb{R}$ y sea $B$ el subconjunto de todas las matrices de la forma

$$\begin{pmatrix} a & a & \dots & a \\ a & a & \dots & a \\ \dots & \dots & \dots & \dots \\ a & a & \dots & a \end{pmatrix}$$

Es fácil comprobar que con a suma y producto usuales de matrices, $B$ es un anillo cuya unidad es la matriz

$$\begin{pmatrix} 1/n & 1/n & \dots & 1/n \\ 1/n & 1/n & \dots & 1/n \\ \dots & \dots & \dots & \dots \\ 1/n & 1/n & \dots & 1/n \end{pmatrix}$$

Pero *$B$ no es un subanillo de $A$* porque no tienen la misma unidad, aunque la suma y el producto sean los mismos.

*Ejemplo* 2.5.15. Para cualquier homomorfismo de anillos $f : A \to B$ el conjunto $\mathrm{Im}(f)$ es un subanillo de $B$.

**Proposición 2.5.16.** *Sea $C$ subanillo de $B$ y sea $B$ subanillo de $A$. Entonces $C$ es un subanillo de $A$.*

Como ilustración del criterio vamos a demostrar:

**Proposición 2.5.17.** *Sea $\{B_\lambda \mid \lambda \in \Lambda\}$ una familia de subanillos de un anillo $A$. Entonces $B = \cap_\lambda B_\lambda$ es un subanillo de $A$.*

Esta proposición nos permite definir dos conceptos importantes:

**Definición 2.5.18.** Sea $S$ un subconjunto de $A$. Llamamos *subanillo generado por* $S$ a la intersección $B$ de todos los subanillos de $A$ que contienen a $S$. Lo representamos por $B = \mathbb{Z}[S]$.

*Ejemplo* 2.5.19. El anillo $\mathbb{J}$ de los enteros de Gauss es el subanillo generado por $i$

**Definición 2.5.20.** Sea $\{B_\lambda \mid \lambda \in \Lambda\}$ una familia arbitraria de subanillos de $A$. Llamamos *compuesto de los* $B_\lambda$ al subanillo generado por $S = \cup_\lambda B_\lambda$.

**Proposición 2.5.21.** *1. Sea $S = \emptyset$. Entonces $\mathbb{Z}[S]$ es el subanillo primo.*

*2. Sea $A$ conmutativo. Para cualquier $S \subset A$ no vacío, $\mathbb{Z}[S]$ es el conjunto de todos los elementos de $A$ que se expresan como polinomios en los elementos de $S$ con coeficientes enteros.*

**Proposición 2.5.22.** *Sea $B$ un subanillo cualquiera de $A$. Entonces $B$ contiene al subanillo primo de $A$.*

En anillos existe otra subestructura importante:

**Definición 2.5.23.** Sea $A$ un anillo y sea $I$ un subconjunto no vacío. Decimos que $I$ es un *ideal* de $A$ si se verifica:

- $I$ es un subgruo de $(A, +)$
- $\forall a \in A\ \forall x \in I\ ax, xa \in I$

*Ejemplo* 2.5.24. Todo anillo tiene dos ideales: El ideal trivial o nulo formado sólo por el elemento 0 y el ideal total que es todo el anillo. Estos son los *ideales impropios*. Cualquier otro ideal es un *ideal propio*.

**Proposición 2.5.25.** *Un ideal $I$ de $A$ contiene al 1 si y sólo si $I = A$*

**Corolario 2.5.26.** *Un ideal $I$ de $A$ es propio si y sólo si no es trivial y $1 \notin I$.*

*Ejemplo* 2.5.27. Para cualquier homomorfismo de anillos $f : A \to B$ el núcleo $\ker(f)$ es un ideal de $A$.

*Ejemplo* 2.5.28. Sea $A$ un anillo conmutativo y sea $a$ un elemento de $A$. El conjunto $Aa = \{xa \mid x \in A\}$ es un ideal de $A$ que se llama *ideal principal generado por* $a$.

**Proposición 2.5.29.** *Sea $\{I_\lambda \mid \lambda \in \Lambda\}$ una familia de ideales de un anillo $A$. Entonces $I = \cap_\lambda I_\lambda$ es un ideal de $A$.*

**Proposición 2.5.30.** *Sean $I, J$ ideales de un anillo $A$. Entonces $I + J$ es un ideal de $A$.*

**Definición 2.5.31.** Sea $S$ un subconjunto del anillo $A$. Llamamos *ideal generado por* $S$ a la intersección de todos los ideales que contienen a $S$. Se representa por $(S)$.

Si $S = \{a_1, \ldots, a_n\}$ es un con junto finito, el ideal generado por $S$ se representa por $(a_1, \ldots, a_n)$.

*Ejemplo* 2.5.32. Si $S = \emptyset$, $(S) = 0$ es el ideal nulo.

*Ejemplo* 2.5.33. Si $A$ es conmutativo y $a \in A$, $(a) = Aa$ el ideal prinicipal generado por $a$.

**Proposición 2.5.34.** *Sea $A$ un anillo conmutativo y $S$ un subconjunto no vacío suyo. Entonces*

$$(S) = \{x = \sum_a x_a a \mid a \in S, x_a \in A\}$$

**Corolario 2.5.35.** *Sea $S = \{a_1, \ldots, a_n\}$. Entonces*

$$(a_1, \ldots, a_n) = \{x_1 a_1 + \cdots + x_n a_n \mid x_i \in A\} = Aa_1 + \cdots + Aa_n.$$

### 2.5.3. Submódulos

Sea $A$ un anillo fijo. Todos los módulos que vamos a considerar son módulos por la izquierda sobre $A$.

**Definición 2.5.36.** Dados dos módulos $(M,+)$ y $(N,+)$, decimos que $N$ *es un submódulo de* $M$, y lo representamos por $N < M$, cuando $N$ es un subconjunto de $M$ y la aplicación de inserción $N \to M$ es un homomorfismo de módulos.

*Ejemplo* 2.5.37. Todo módulo $M$ tiene dos submódulos: El módulo formado sólo por el elemento cero, que es el *submódulo trivial*, y el mismo $M$, que es el *submódulo total*. Ambos son los *submódulos impropios*. Cualquier otro submódulo es un *submódulo propio*.

Por abuso de lenguaje se suele identificar al submódulo $(N,+)$ con el subconjunto $N$, ya que la ley de composición está determinada por el módulo $N$.

**Proposición 2.5.38** (Caracterizaciones de submódulo)**.** *1. Sea $M$ un módulo y sea $\emptyset \neq N \subset M$. Entonces $N$ es un submódulo de $M$ si y sólo si se verifica:*

a) *Para todo par de elementos $x, y \in N$ también $x + y \in N$.*

b) *Para todo $a \in A$ y todo $x \in N$ también $ax \in N$.*

*2. Sea $M$ un módulo y sea $\emptyset \neq N \subset M$. Entonces $N$ es un submódulo de $M$ si y sólo si se verifica: Para todo par de escalares $a, b \in A$ y todo par de elementos $x, y \in N$ también $ax + by \in N$.*

*Ejemplo* 2.5.39. Para cualquier homomorfismo de módulos $f : M \to N$, el conjunto $\ker(f)$ es un submódulo de $M$ y el conjunto $\mathrm{Im}(f)$ es un submódulo de $N$.

**Proposición 2.5.40.** *Sea $L$ submódulo de $N$ y sea $N$ submódulo de $M$. Entonces $L$ es un submódulo de $M$.*

Como ilustración del criterio vamos a demostrar:

**Proposición 2.5.41.** *Sea $\{N_\lambda \mid \lambda \in \Lambda\}$ una familia de submódulos de un módulo $M$. Entonces $N = \cap_\lambda N_\lambda$ es un submódulo de $M$.*

Esta proposición nos permite definir dos conceptos importantes:

**Definición 2.5.42.** Sea $S$ un subconjunto de $M$. Llamamos *submódulo generado por* $S$ a la intersección $N$ de todos los submódulos de $M$ que contienen a $N$. Lo representamos por $N = A\langle S\rangle$.

**Proposición 2.5.43.** *Sean $N_1, N_2$ submódulos de $M$. Entonces $N_1 + N_2$ es un submódulo de $M$.*

**Proposición 2.5.44.** *1. Sea $S = \emptyset$. Entonces $\langle S\rangle$ es el submódulo trivial.*

*2. Para cualquier $S \subset M$ no vacío,*

$$A\langle S\rangle = \{\sum a_x x \mid a_x \in A \text{ casi todos cero},\ x \in S\}$$

*es el conjunto de todos los elementos de $G$ que se expresan como combinaciones lineales finitas de elementos de $S$ con coeficientes en $A$.*

## 2.6. Anillos cocientes

Sean $A$ un anillo e $I$ un ideal suyo. Definimos una relación binaria en $A$ por la regla

$$a \sim b \Leftrightarrow a - b \in I \tag{2.6.1}$$

**Lema 2.6.1.** *La relación 2.6.1 es una relación de equivalencia.*

Representamos por $\overline{a} = a + I$ a la clase de equivalencia del elemento $a \in A$. Cualquier elemento de $\overline{a}$ se llama *representante de la clase* $\overline{a}$. Representamos por $A/I$ al conjunto de todas las clases de equivalencia para la relación 2.6.1. En $A/I$ definimos dos operaciones internas:

$$\overline{a} + \overline{b} = \overline{a+b} \tag{2.6.2}$$

$$\overline{a}\overline{b} = \overline{ab} \tag{2.6.3}$$

**Lema 2.6.2.** *Sean* $\overline{a} = \overline{a_1}$ *y* $\overline{b} = \overline{b_1}$. *Entonces* $\overline{a+b} = \overline{a_1 + b_1}$ *y* $\overline{ab} = \overline{a_1 b_1}$

Este lema nos dice que las operaciones 2.6.2 están bien definidas, es decir que son independientes de los representantes elegidos.

**Proposición 2.6.3.** *El conjunto $A/I$ junto con las operaciones 2.6.2 forman un anillo que se llama* anillo cociente de $A$ sobre $I$.

Llamamos *poyección de $A$ sobre $A/I$* a la aplicación $p : A \to A/I$ dada por $p(a) = \overline{a}$.

**Proposición 2.6.4.** *La proyección $p : A \to A/I$ es un epimorfismo de anillos con núcleo* $\ker(p) = I$.

**Corolario 2.6.5.** *Un subconjunto $I \subset A$ es un ideal si y sólo si existe un homomorfismo de anillos $f : A \to B$ tal que $I = \ker f$.*

**Teorema 2.6.6** (Propiedad universal del anillo cociente)**.** *Sean $A$ un anillo e $I$ un ideal suyo. Para todo homomorfismo de anillos $f : A \to B$ tal que* $\ker f \supset I$ *existe un único homomorfismo de anillos $\overline{f} : A/I \to B$ tal que $\overline{f}p = f$.*

*Además* $\operatorname{Im} \overline{f} = \operatorname{Im}(f)$ *y* $\overline{a} \in \ker(\overline{f})$ *si y sólo si* $a \in \ker(f)$.

**Corolario 2.6.7.** *$\overline{f}$ es un epimorfismo si y sólo si $f$ es un epimorfismo.*

*$\overline{f}$ es un monomorfismo si y sólo si $I = \ker(f)$.*

**Proposición 2.6.8** (Descomposición canónica de un homomorfismo)**.** *Todo homomorfismo de anillos $f : A \to B$ se descompone como un producto*

$$A \xrightarrow{f_1} \frac{A}{\ker(f)} \xrightarrow{f_2} \operatorname{Im}(f) \xrightarrow{f_3} B$$

*donde $f_1$ es un epimorfismo, $f_2$ es un isomorfismo y $f_3$ es un monomorfismo.*

**Corolario 2.6.9** (Primer teorema de isomorfismo)**.** *Para todo homomorfismo de anillos $f : A \to B$ existe un isomorfismo* $A/\ker(f) \cong \operatorname{Im}(f)$ *dado por* $\overline{a} \leftrightarrow f(a)$.

**Teorema 2.6.10** (Teorema de correspondencia)**.** *Sean $A$ un anillo e $I$ un ideal suyo y sea $p : A \to A/I$ la proyección. Sean*

$$S = \{U \mid U \text{ es un subgrupo aditivo de } A \text{ y } U \supset I\}$$
$$S_I = \{V \mid V \text{ es un subgrupo aditivo de } A/I\}$$

1. *La aplicación $U \to p(U) = U/I$ establece una biyección $S \cong S_I$.*
2. *En esta biyección $S \subset T$ si y sólo si $p(S) \subset p(T)$.*
3. *$S$ es un subanillo de $A$ si y sólo si $p(S)$ es un subanillo de $A/I$.*
4. *$S$ es un ideal de $A$ si y sólo si $p(S)$ es un ideal de $A/I$.*

**Teorema 2.6.11** (Segundo teorema de isomorfismo)**.** *Sea $A$ un anillo y sean $B$ un subanillo e $I$ un ideal de $A$. Entonces:*

1. *$B + I = \{b + x \mid b \in B,\ x \in I\}$ es un subanillo de $A$ e $I$ es un ideal de $B + I$.*
2. *$B \cap I$ es un ideal de $B$*
3. *Existe un isomorfismo*
$$\frac{B}{B \cap I} \cong \frac{B + I}{I}$$
*dado por $b + B \cap I \leftrightarrow b + I$.*

**Teorema 2.6.12** (Tercer teorema de isomorfismo)**.** *Sea $A$ un anillo y sean $I \supset J$ ideales suyos. Entonces $I/J$ es un ideal de $A/J$ y existe un isomorfismo*
$$\frac{A/J}{I/J} \cong \frac{A}{I}$$

## 2.7. Dominios de integridad y cuerpos

Sea $A$ un anillo conmutativo.

**Definición 2.7.1.** Un elementos $a \in A$ se llama *divisor de cero* si existe un $b \in A$, $b \neq 0$ tal que $ab = 0$.
Un *dominio de integridad* es un anillo conmutativo $A$ no trivial sin divisores de cero no nulos.

En otras palabras, un anillo conmutativo $A$ es un dominio de integridad si $1 \neq 0$ y si $ab = 0 \Rightarrow a = 0$ o $b = 0$.

**Proposición 2.7.2.** *Un anillo conmutativo no trivial $A$ es un dominio de integridad si y sólo si satisface la* ley cancelativa*:*
$$ab = ac \text{ y } a \neq 0 \Rightarrow b = c$$

**Corolario 2.7.3.** *Sea $A$ un dominio de integridad y sea $B$ un subanillo de $A$. Entonces $B$ es un dominio de integridad.*

**Definición 2.7.4.** Un *cuerpo* es un anillo conmutativo no trivial en el que todo elemento no nulo tiene un inverso multiplicativo.
Un *subcuerpo* de un cuerpo $F$ es un subanillo que es un cuerpo.

En otras palabras, el cuerpo $K$ es un subcuerpo de $F$ si y sólo si es un subconjunto y la aplicación de inclusión $i : K \to F$ es un homomorfismo.

**Lema 2.7.5.** *Un subconjunto de un cuerpo $F$ es un subcuerpo si y sólo si es cerrado para la suma, la multiplicación, el cero, el uno, el opuesto aditivo y el inverso multiplicativo.*

**Proposición 2.7.6.** *Todo cuerpo es un dominio de integridad.*

**Proposición 2.7.7.** *Todo dominio de integridad finito es un cuerpo.*

**Proposición 2.7.8.** *Un anillo conmutativo no trivial es un cuerpo si y solo si no tiene ideales propios.*

**Corolario 2.7.9.** *Todo homomorfismo de cuerpos $K \to F$ es inyectivo.*

**Definición 2.7.10.** Sea $A$ un anillo conmutativo. Un ideal $I$ de $A$ se llama *maximal* si $I \neq A$ y si para $J$ ideal de $A$, $I \subset J \Rightarrow J = I$ o $J = A$.

Un ideal $I$ de $A$ se llama *primo* si $I \neq A$ y si para $a, b \in A$ $ab \in I \Rightarrow a \in I$ o $b \in I$.

**Proposición 2.7.11.** *Sea $A$ un anillo conmutativo y sea $I$ un ideal suyo. El ideal $I$ es maximal si y sólo si el anillo cociente $A/I$ es un cuerpo.*

*El ideal $I$ es primo si y sólo si el anillo cociente $A/I$ es un dominio de integridad.*

**Corolario 2.7.12.** *Todo ideal maximal es primo.*

**Definición 2.7.13.** Un *anillo de integridad* o *anillo íntegro* es un anillo (no necesariamente conmutativo) sin divisores de cero.

Un *anillo de división* es un anillo (no necesariamente conmutativo) en el que todo elemento distinto de cero tiene un inverso.

Así que un dominio de integridad es lo mismo que un anillo de integridad conmutativo y un cuerpo es lo mismo que un anillo de división conmutativo. Naturalmente todo anillo de división es un anillo de integridad.

**Proposición 2.7.14.** *La característica de un dominio de integridad es o cero o un número primo.*

**Proposición 2.7.15.** *Sea $K$ un cuerpo. La intersección de una familia arbitrarias de subcuerpos de $K$ es un subcuerpo de $K$.*

**Definición 2.7.16.** Sea $K$ un cuerpo. Se llama *subcuerpo primo* de $K$ a la intersección de todos los subcuerpos de $K$.

Es decir, que el subcuerpo primo es el mínimo subcuerpo de $K$.

## 2.8. El cuerpo de fracciones

Sea $A$ un dominio de integridad. Llamamos $S$ al conjunto de elementos no nulos de $A$. En el conjunto producto cartesiano $S \times A$ definimos la siguiente relación binaria:

$$(s_1, a_1) \sim (s_2, a_2) \Leftrightarrow s_1 a_2 = s_2 a_1 \tag{2.8.1}$$

**Proposición 2.8.1.** *La relación 2.8.1 es una relación de equivalencia.*

Al conjunto cociente $S \times A/\sim$ lo representamos por $Q(A)$ o por $S^{-1}A$. En este conjunto la clase De $(s, a)$ se representa por $a/s$ y se llama *fracción*; el elemento $a$ es el *numerador* y $s$ es el *denominador* de la fracción.

Definimos dos operaciones binarias $Q(A) \times Q(A) \to Q(A)$ por las reglas:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{s_2 a_1 + s_1 a_2}{s_1 s_2} \tag{2.8.2}$$

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2} \tag{2.8.3}$$

**Proposición 2.8.2.** *Las operaciones 2.8.2 y 2.8.3 están bien definidas (es decir, son independientes de los representantes elegidos para las fracciones).*

**Proposición 2.8.3.** *El conjunto $Q(A)$ con las operaciones 2.8.2 y 2.8.3 es un cuerpo que se llama* cuerpo de fracciones *del anillo $A$.*

*Ejemplo* 2.8.4. Cuando $A = \mathbb{Z}$, el cuerpo de fracciones es el *cuerpo de los números racionales* $Q(A) = \mathbb{Q}$.

*Ejemplo* 2.8.5. $\mathbb{Q}(\sqrt{2})$ es el cuerpo de fracciones de $\mathbb{Z}[\sqrt{2}]$.

*Ejemplo* 2.8.6. $\mathbb{Q}(\sqrt{-1}) = \{a + bi \mid a, b \in \mathbb{Q}\}$ es el cuerpo de fracciones del anillo de los enteros de Gauss $\mathbb{J} = \mathbb{Z}[i]$.

El anillo $A$ determina unívocamente al cuerpo $Q(A)$ (salvo isomorfismos). Pero para un cuerpo $K$ puede ocurrir que $K = Q(A) = Q(B)$ aunque $A$ y $B$ no sean isomorfos:

*Ejemplo* 2.8.7. Sea $B = \{a/b \in \mathbb{Q} \mid b \equiv 1 \pmod 2\}$. Es fácil ver que $Q(B) = \mathbb{Q}$, aunque $B \ncong \mathbb{Z}$.

**Proposición 2.8.8.** *La aplicación $\lambda : A \to Q(A)$ definida por $\lambda(a) = a/1$ es un monomorfismo de anillos.*

Usualmente se identifica el anillo $A$ con la imagen del anterior monomorfismo, es decir que tomamos $a = a/1$. Con esta identificación $A$ es un subanillo de $Q(A)$.

**Lema 2.8.9.** *Todo dominio de integridad es un subanillo de algún cuerpo.*

Este resultado es falso para anillos de integridad: Malcev ha dado ejemplos de anillos de integridad que no se pueden sumergir en un anillo de división.

**Teorema 2.8.10.** *Para todo monomorfismo $f : A \to K$ donde $K$ es un cuerpo existe un único homomorfismo $\bar{f} : Q(A) \to K$ tal que $\bar{f}\lambda = f$. Además* $\mathrm{Im}(\bar{f}) \cong Q(A)$.

**Corolario 2.8.11.** *Sea $A$ un subanillo de un cuerpo $K$ tal que todo elemento $u \in K$ se puede expresar como $u = ab^{-1}$ con $a, b \in A$. Entonces $Q(A) \cong K$.*

**Proposición 2.8.12.** *Sea $K$ un cuerpo. Si $car(K) = 0$, el cuerpo primo de $K$ es isomorfo a $\mathbb{Q}$. Si $car(K) = p$, el cuerpo primo es isomorfo a $\mathbb{Z}_p$.*

## 2.9. Factorización

Sea $A$ un dominio de integridad y sean $a, b \in A$.

**Definición 2.9.1.** Decimos que *$b$ es un múltiplo de $a$* y que *$a$ divide a $b$* si existe un $c \in A$ tal que $ac = b$. Se representa por $a \mid b$.

Todo divisor de 1 se llama *unidad* del anillo $A$.

Dos elementos $a, b \in A$ se llaman *asociados* si $a$ divide a $b$ y $b$ divide a $a$.

Para un anillo $A$, el conjunto de divisores de uno constituye un grupo multiplicativo que se llama *grupo de las unidades* y se representa por $A^\times$.

*Ejemplo* 2.9.2. $\mathbb{Z}^\times = \{1, -1\}$.
$\mathbb{J}^\times = \{1, i, -1, -i\}$.
$\mathbb{Z}[\sqrt{2}]^\times = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z},\ a^2 - 2b^2 = \pm 1\}$.

**Lema 2.9.3.** *En un dominio de integridad $A$ dos elementos $a, b \in A$ son asociados si y sólo si existe una unidad $u \in A$ tal que $a = bu$.*

**Definición 2.9.4.** Un elemento $a \in A$ es un *irreducible* o *átomo* de $A$ si no es una unidad y si $a = bc$ implica que $b$ o $c$ es una unidad.

*Ejemplo* 2.9.5. En $\mathbb{Z}$ las unidades son 1 y $-1$ y los irreducibles son los primos y sus negativos.

Sea $A$ un dominio de integridad y sean $a, b \in A$.

**Definición 2.9.6.** Un *máximo común divisor* de $a$ y $b$ es un elemento $d \in A$ que verifica dos propiedades:

1. $d \mid a$ y $d \mid b$.
2. Para $c \in A$, $c \mid a$ y $c \mid b \Rightarrow c \mid d$.

Se suele representar $d = (a, b) = \text{m. c. d.}(a, b)$.

**Lema 2.9.7.** *Dos máximos comunes divisores $d, d'$ de $a$ y $b$ son asociados.*

**Definición 2.9.8.** Dos elementos $a, b \in A$ son *primos relativos* si $\text{m. c. d.}(a, b) = 1$.

**Proposición 2.9.9.** *Sea $A$ un dominio de integridad y sean $a, b, c \in A$. Las siguientes reglas se verifican siempre que existan los máximos comunes divisores implicados:*

1. $(a, b) = (b, a)$
2. $((a, b), c) = (a, (b, c))$
3. $(ac, bc) = (a, b)c$
4. $(a, b)$ *es asociado de $a$ si y sólo si $a \mid b$.*
5. $(a, 0) = a$.

**Definición 2.9.10.** Sea $A$ un dominio de integridad. Un *mínimo común múltiplo* de $a$ y $b$ es un elemento $m \in A$ que verifica dos propiedades:

1. $a \mid m$ y $b \mid m$.
2. Para $c \in A$, $a \mid c$ y $b \mid c \Rightarrow m \mid c$.

Se suele representar $m = [a, b] = \text{m. c. m.}(a, b)$.

**Lema 2.9.11.** *Dos mínimos comunes múltiplos $m, m'$ de $a$ y $b$ son asociados.*

**Proposición 2.9.12.** *Sea $A$ un dominio de integridad y sean $a, b, c \in A$. Las siguientes reglas se verifican siempre que existan los mínimos comunes múltiplos implicados*

1. $[a, b] = [b, a]$
2. $[[a, b], c] = [a, [b, c]]$
3. $[ac, bc] = [a, b]c$
4. $[a, b]$ *es asociado de $a$ si y sólo si $b \mid a$.*
5. $[a, 1] = a$.

**Proposición 2.9.13.** *Sea $A$ un dominio de integridad y sean $a, b$ dos elementos de $A$ que tienen un mínimo común múltiplo $m$. Entonces $m = 0$ si y sólo si $a = 0$ o $b = 0$. Si $m \neq 0$, el elemento $d = ab/m$ es un máximo común divisor de $a$ y $b$.*

*Demostración.* Sea $ab \neq 0$. El producto $ab$ es un múltiplo de $a$ y $b$, luego $m \mid ab$. Sea $ab = md$. En particular $m \neq 0$. Además $m = ab_1 = a_1 b$, así que $ab = ab_1 d = a_1 bd$. Como $A$ es un dominio de integridad, $b = b_1 d$ y $a = a_1 d$, luego $d$ divide a $a$ y $b$. Sea $d_1$ otro divisor común de $a$ y $b$. Llamamos $m_1 = ab/d_1$. Es fácil ver que $m_1$ es un múltiplo común de $a$ y $b$, luego existe $c \in A$ tal que $m_1 = mc$. De donde $md = ab = m_1 d_1 = mcd_1$. Luego $d = cd_1$ y $d_1$ es un divisor de $d$. □

El enunciado recíproco es falso:

*Ejemplo* 2.9.14. Sea $A$ el subanillo de $\mathbb{Z}[X]$ formado por los polinomios con coeficiente de $X$ par. Los elementos 2 y $2X$ tienen un máximo común divisor en $A$, pero no tienen mínimo común múltiplo.

Sin embargo es cierto cuando *todos* los pares tienen un máximo común divisor:

**Proposición 2.9.15.** *Sea $A$ un dominio de integridad en el que todo par de elementos tiene un máximo común divisor. Entonces todo par de elementos tiene un mínimo común múltiplo.*

*Demostración.* Sean $a, b \in A$, $ab \neq 0$. Sea $d = \text{m. c. d.}(a, b)$, así que $a = a_1 d$ y $b = b_1 d$ con $a_1, b_1 \in A$. Sea $m = ab/d = a_1 b_1 d = ab_1 = a_1 b$. Evidentemente $a \mid m$ y $b \mid m$. Sea $m_1$ un múltiplo común arbitrario de $a, b$ y sea $k = \text{m. c. d.}(m, m_1)$. Como $a$ y $b$ son divisores de $m$ y $m_1$, necesariamente $a$ y $b$ dividen a $k$. Sea $m = kd_1$ y sea $k = au = bv$. Sustituyendo obtenemos $a_1 b = m = kd_1 = bvd_1$. Simplificando nos queda $a_1 = vd_1$ y por tanto $a = a_1 d = v(d_1 d)$. Similarmente $b = u(d_1 d)$. Por tanto $(d_1 d)$ divide a $\text{m. c. d.}(a, b) = d$. Sea $d = cd_1 d$. Simplificando nos queda $1 = cd_1$, por lo que $d_1$ es una unidad y $k, m$ son asociados, así que $m$ divide a $m_1$.Luego $m = \text{m. c. m.}(a, b)$. □

## 2.9.1. Dominios de factorización única

El *teorema fundamental de la aritmética* dice que todo entero se factoriza en irreducibles de forma esencialmente única. La unicidad de la factorización resulta ser muy útil, lo que motiva la siguiente definición.

**Definición 2.9.16.** Un *dominio de factorización única* (abreviadamente, un DFU) o *dominio factorial* es un dominio de integridad en el que todo elemento no nulo ni unidad se puede escribir como un producto de irreducibles y además verifica que dadas dos factorizaciones en irreducibles del mismo elemento

$$a = p_1 \dots p_n = q_1 \dots q_m$$

entonces $n = m$ y existe una permutación $\sigma \in S_n$ tal que $p_i$ es asociado de $q_{\sigma(i)}$ para $i = 1, \dots, n$.

*Ejemplo* 2.9.17. $\mathbb{Z}$ es un dominio de factorización única por el teorema fundamental de la aritmética.

*Ejemplo* 2.9.18. Todo cuerpo es un dominio de factorización única de manera trivial.

Mas adelante veremos que los anillos de polinomios con coeficientes en un dominio de factorización única también son dominio de factorización única.

Sea $A$ un dominio de factorización única y sea $\mathcal{P}$ un conjunto de irreducibles tal que todo irreducible de $A$ está asociado exactamente a un irreducible de $\mathcal{P}$. (en muchos ejemplos interesantes $\mathcal{P}$ es infinito, pero esto no es esencial). Todo elemento $a$ de $A$ se escribe de manera única como $a = up_1^{k_1} \dots p_n^{k_n}$ donde $u$ es una unidad y los $p_i$ son elementos de $\mathcal{P}$.

**Lema 2.9.19.** *Sean $a = up_1^{k_1} \dots p_n^{k_n}$ y $b = up_1^{t_1} \dots p_n^{t_n}$ elementos de $A$. Entonces $a \mid b$ si y sólo si $k_1 \leq t_i$ para $i = 1, \dots, n$*

**Proposición 2.9.20.** *Sea $A$ un dominio de factorización única, sean $a, b \in A$ y sean $a = up_1^{k_1} \dots p_n^{k_n}$ y $b = up_1^{t_1} \dots p_n^{t_n}$ las factorizaciones en irreducibles. Entonces $\text{m. c. d.}(a, b) = up_1^{l_1} \dots p_n^{l_n}$ donde $l_i = \min(k_i, t_i)$ para $i = 1, \dots, n$.*

**Proposición 2.9.21.** *Sea $A$ un dominio de factorización única Sean $a = up_1^{k_1} \dots p_n^{k_n}$ y $b = up_1^{t_1} \dots p_n^{t_n}$ las factorizaciones en irreducibles. Entonces $\text{m. c. m.}(a, b) = up_1^{s_1} \dots p_n^{s_n}$ donde $s_i = \max(k_i, t_i)$ para $i = 1, \dots, n$.*

Vamos a establecer dos caracterizaciones de los dominios de factorización única.

**Definición 2.9.22.** Sea $A$ un dominio de integridad y $p$ un elemento suyo; $p$ es un *elemento primo* de $A$ si no es cero ni unidad y para $a, b \in A$ se verifica que $p \mid ab$ si y sólo si $p \mid a$ o $p \mid b$.

*Ejemplo* 2.9.23. Los primos de $\mathbb{Z}$ son los números primos y sus opuestos.

**Lema 2.9.24.** *Sea $p$ un primo de $A$ y sean $a_1, \ldots, a_n \in A$. Entonces $p$ divide al producto $a_1 \ldots a_n$ si y sólo si existe un $i$ tal que $p \mid a_i$.*

**Lema 2.9.25.** *Todo primo es un irreducible.*

**Teorema 2.9.26.** *Un dominio de integridad $A$ es un dominio de factorización única si y sólo si*

1. *Todo elemento no nulo ni unidad descompone como producto de irreducibles*
2. *Todo irreducible es primo.*

*Demostración.* Sea $A$ un dominio de factorización única y sea $u \in A$ irreducible Sean $a, b \in A$ tales que $u \mid ab$. Entonces existe un $c \in A$ tal que $uc = ab$. Sean $a = u_1 \ldots u_n$, $b = u_{n+1} \ldots u_m$ y $c = v_1 \ldots v_k$ factorizaciones en irreducibles Sustituyendo nos queda $uv_1 \ldots v_k = u_1 \ldots v_m$. Estas son dos factorizaciones en irreducibles. Como $A$ es factorial, $k + 1 = m$ y existe un $u_j$ asociado con $u$. Si $j \leq n$, resulta que $u \mid a$ y si $j > n$ queda que $u \mid b$. Luego $u$ es primo.

A la inversa, sea $A$ un dominio de integridad verificando las condiciones del enunciado y sean $a = p_1 \ldots p_n = q_1 \ldots q_m$ dos factorizaciones en irreducibles. Si n=1, $p_1 = q_1 \ldots q_m$ y como $p_1$ es irreducible, necesariamente $m = n$ y $p_1 = q_1$.

Sea ahora $n > 1$ y supongamos que la factorización es única siempre que uno de los productos tenga menos de $n$ factores. Como $p_1 \mid q_1 \ldots q_m$ y $p_1$ es primo, existe un $q_j$ tal que $p_1 \mid q_j$ y como $q_j$ es irreducible, $q_j = p_1 u$ con $u$ invertible. Por sencillez suponemos que $j = 1$. Nos queda $p_1 \ldots p_n = p_1(uq_2) \ldots q_m$ y simplificando $p_2 \ldots p_n = (uq_2) \ldots q_m$. Pero ahora el primer miembro tiene $n - 1$ factores. Por la hipótesis de inducción, $n - 1 = m - 1$ y existe una permutación $i \mapsto j$ ta que $p_i$ y $q_j$ son asociados. □

**Teorema 2.9.27.** *Un dominio de integridad $A$ es un dominio de factorización única si y sólo si*

1. *Todo elemento no nulo ni unidad descompone como producto de irreducibles*
2. *Todo par de elementos tiene máximo común divisor.*

*Demostración.* La primera condición es la misma en ambos casos. Sea $A$ un dominio de factorización única. Por la proposición 2.9.20 todo par de elementos tiene un máximo común divisor.

A la inversa, supongamos que todo par de elementos tiene un máximo común divisor. Sea $u \in A$ un irreducible arbitrario y sean $a, b \in A$ tales que $u \nmid a$ y $u \nmid b$, es decir que $\text{m. c. d.}(u, a) = 1 = \text{m. c. d.}(u, b)$. Por la proposición 2.9.9, $b = (ub, ab)$ y $1 = (u, b) = (u, (ub, ab)) = ((u, ub), ab) = (u(1, b), ab) = (u, ab)$. El contrarrecíproco nos dice que $(u, ab) = u \Rightarrow (u, a) = u$ ó $(u, b) = u$ □

Las proposiciones 2.9.20 y 2.9.21 suministran una forma cómoda de calcular el máximo común divisor y el mínimo común múltiplo. La pega es que presuponen que $A$ es un dominio de factorización única y que $a$ y $b$ han sido factorizados en $A$. Pero el proceso de factorizar completamente un elemento normalmente es largo y penoso. Para $\mathbb{Z}$, $K[X]$ y otros dominios de integridad existe un método mas directo y efectivo de calcular el máximo común divisor usando un algoritmo de división con resto. Esto motiva la definición de dos nuevas clases de anillos: Los dominios de ideales principales y los dominios euclídeos.

### 2.9.2. Dominios de ideales principales

**Definición 2.9.28.** Un *dominio de ideales principales* (abreviado por D.I.P) es un dominio de integridad en el que todo ideal es principal.

**Lema 2.9.29.** *En un dominio de ideales principales $A$ toda cadena ascendente de ideales*

$$(a_1) \subset (a_2) \subset \dots$$

*es estacionaria, es decir que existe un $n$ tal que $(a_n) = (a_{n+1}) = \dots$:*

*Demostración.* Sea $I = \cup_i(a_i)$. Es fácil comprobar que $I$ es un ideal de $A$, luego existe un $b \in I$ tal que $I = (b)$. Como $I$ es la unión de los ideales $(a_i)$, existe un $n$ tal que $b \in (a_n)$, es decir que $b = ca_n$ es un múltiplo de $a_n$. Para cualquier $m$ tenemos que $a_m \in I$, luego $a_m = d_m b$ es un múltiplo de $b$. Sustituyendo tenemos que $a_m = d_m c a_n \in (a_n)$ y por tanto $(a_m) \subset (a_n)$ para todo $m$. Luego $(a_m) = (a_n)$ para todo $m \geq n$. □

**Proposición 2.9.30.** *Todo dominio de ideales principales es un dominio de factorización única.*

*Demostración.*

1. *Todo elemento de un dominio de ideales principales se descompone como producto de irreducibles:*

   Sea $A$ un dominio de ideales principales arbitrario y sea $a_1 \in A$ cualquier elemento que no es invertible. Si $a_1$ es irreducible, tenemos una factorización $a_1 = p_1$. Si $a_1$ es reducible existe una factorización $a_1 = a_2 b_1$ con $a_2$ y $b_1$ no invertibles, y por tanto $(a_1) \subsetneq (a_2)$. Si $a_2$ es reducible, repetimos el razonamiento y obtenemos un $a_3$ no invertible tal que $(a_1) \subsetneq (a_2) \subsetneq (a_3)$. Por el lema anterior, este proceso no puede ser infinito. Luego llegamos a una factorización $a_1 = p_1 a_2$ con $p_1$ irreducible.

   Si $a_2$ es irreducible o invertible, tenemos una factorización de $a_1$ en irreducibles. En otro caso, repetimos el proceso y obtenemos $a_2 = p_2 a_3$ con $p_2$ irreducible y $a_1 = p_1 p_2 a_3$. Otra vez tenemos una cadena ascendente de ideales $(a_1) \subsetneq (a_2) \subsetneq (a_3) \dots$. Por el lema anterior, esta cadena es estacionaria. Luego existe un $n$ tal que $a_1 = p_1 \dots p_n$ es una factorización de $a_1$ como producto de irreducibles.

2. *En un dominio de ideales principales $A$ todo par de elementos tiene un máximo común divisor:*

   Sean $a, b \in A$ arbitrarios y sea $I = (a, b)$ el ideal generado por ellos. Por ser $A$ un dominio de ideales principales, existe un $d \in I$ tal que $(a, b) = (d)$. Los elementos $a, b$ están en $I = (d)$ luego $d \mid a$ y $d \mid b$. Además existen $u, v \in A$ tales que $d = ua + vb$. Sea $c$ un divisor común de $a$ y $b$, así que $a = a_1 c$ y $b = b_1 c$. Luego $d = ua_1 c + vb_1 c = (ua_1 + vb_1)c$ es un múltiplo de $c$.

□

**Corolario 2.9.31** (Identidad de Bezout)**.** *Sea $A$ un dominio de ideales principales. Para cualesquiera $a, b \in A$ existen $u, v \in A$ tales que*

$$d = \text{m. c. d.}(a, b) = ua + vb$$

# Capítulo 3

# Dominios Euclídeos

## 3.1. Definiciones y resultados básicos

**Definición 3.1.1.** Sea $A$ un dominio de integridad. Una *función euclídea* es una función $\phi : A - \{0\} \to \mathbb{Z}^+$ que verifica

1. Para cualesquiera $a, b \in A$ con $ab \neq 0$ se tiene $\phi(ab) \geq \phi(a)$.

2. Para cualesquiera $a, b \in A$ con $b \neq 0$ existen $q, r \in A$ tales que $a = bq + r$ y o bien $\phi(r) < \phi(b)$ o bien $r = 0$.

Un dominio de integridad que tenga una función euclídea se llama *dominio euclídeo*.

*Ejemplo* 3.1.2. El anillo $\mathbb{Z}$ de los enteros es un dominio euclídeo tomando la función $\phi(n) = |n|$.

Generalmente para verificar que un anillo es euclídeo es mas conveniente reemplazar la segunda condición por otra:

**Lema 3.1.3.** *La segunda condición de la definición de función euclídea es equivalente a la siguiente: Para cualesquiera $a, b \in A$ si $\phi(a) \geq \phi(b)$ existe un $c \in A$ tal que $\phi(a - bc) < \phi(a)$ o $a = bc$.*

*Ejemplo* 3.1.4. Sea $K$ un cuerpo arbitrario. El anillo de polinomios $K[X]$ es un anillo euclídeo para la función $\phi(f) = gr(f)$.

La siguiente propiedad es la que hace muy fácil trabajar con los anillos euclídeos:

**Teorema 3.1.5.** *Todo anillo euclídeo es un dominio de ideales principales.*

*Demostración.* Sea $A$ un dominio euclídeo y sea $I$ un ideal de $A$. Si $I \neq 0$ existe un $a \in I$, $a \neq 0$, con $\phi(a)$ mínimo. Entonces $(a) \subset I$.

Supongamos que $(a) \subsetneq I$. Sea $b \in I$, $b \notin (a)$. Dividimos $b = qa + r$. Ahora $r = b - qa \in I$, $r \neq 0$ y $\phi(r) < \phi(a)$ en contradicción con la elección de $a$. Luego $(a) = I$. □

**Corolario 3.1.6** (Teorema de Bezout)**.** *En un anillo euclídeo $A$ dos elementos cualesquiera $a, b \in A$ tienen un máximo común divisor $d$ y existen $u, v \in A$ tales que*

$$d = au + bv$$

*Demostración alternativa (Algoritmo extendido de Euclides):* Sea $\phi(a) \geq \phi(b)$ y aplicamos repetidamente la propiedad 3.1.3. Tras un número finito de pasos tenemos un resto cero:

$$\begin{aligned} a &= bq_1 + r_1 \qquad \phi(r_1) < \phi(b) \\ b &= r_1q_2 + r_2 \qquad \phi(r_2) < \phi(r_1) \\ &\dots \qquad \dots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n \qquad \phi(r_n) < \phi(r_{n-1}) \\ r_{n-1} &= r_nq_n \qquad r_{n+1} = 0 \end{aligned}$$

porque $\phi(b) > \phi(r_1) > \dots$ es una sucesión estrictamente decreciente de números no negativos que debe pararse y esto sólo puede ocurrir cuando un resto es cero.

De la primera ecuación vemos que $r_1$ es de la forma $ax + by$ con $x, y \in A$. Por inducción lo mismo se verifica para todo $r_i$: Sean

$$\begin{aligned} r_{i-2} &= ax' + by' \\ r_{i-1} &= ax + by \end{aligned}$$

Entonces $r_i = -r_{i-1}q_i + r_{i-2} = a(x' - xq_i) + b(y' - yq_i)$. En particular

$$r_n = au + bv \tag{3.1.1}$$

Además $r_n$ divide a $r_n$ y a $r_{n-1}$, luego divide a $r_{n-2}$. Por inducción obtenemos que $r_n$ divide $a$ y $b$. Pero de la expresión 3.1.1 cualquier divisor de $a$ y $b$ también divide a $r_n$. Luego $d = r_n = \text{m. c. d.}(a, b)$ □

**Corolario 3.1.7.** *En un anillo euclídeo dos elementos cualesquiera tienen un mínimo común múltiplo.*

**Corolario 3.1.8.** *En un dominio euclídeo todo irreducible es primo.*

**Corolario 3.1.9.** *Todo dominio euclídeo es un dominio de factorización única.*

**Corolario 3.1.10.** *Para cualquier cuerpo $K$ el anillo de polinomios $K[X]$ es un dominio de factorización única.*

## 3.2. Ejemplos: Anillos cuadráticos

### 3.2.1. Cuerpos cuadráticos de números

Sea $D$ un número racional que no es un cuadrado perfecto en $\mathbb{Q}$. Definimos el subconjunto de $\mathbb{C}$

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

Está claro que este subconjunto es cerrado para la resta y la identidad

$$(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D})$$

muestra que también es cerrado para la multiplicación. Por tanto $\mathbb{Q}[\sqrt{D}]$ es un subanillo de $\mathbb{C}$ (e incluso de $\mathbb{R}$ cuando $D > 0$), así que en particular es un anillo conmutativo. Es fácil comprobar que la hipótesis de que $D$ no es un cuadrado implica que todo elemento de $\mathbb{Q}[\sqrt{D}]$ se escribe de manera única como $a + b\sqrt{D}$. También implica que si $a, b$ no son ambos cero, entonces $a^2 - b^2D \neq 0$ y como $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2D$ tenemos que

$$(a + b\sqrt{D})^{-1} = \frac{a}{a^2 - b^2D} - \frac{b}{a^2 - b^2D}\sqrt{D} \in \mathbb{Q}(\sqrt{D})$$

Esto demuestra que todo elemento no nulo de $\mathbb{Q}[\sqrt{D}]$ tiene un inverso en $\mathbb{Q}[\sqrt{D}]$ y por tanto $\mathbb{Q}[\sqrt{D}]$ es un cuerpo, que se llama *cuerpo cuadrático*.

El número racional $D$ puede expresarse como $D = f^2D'$ para algún $f \in \mathbb{Q}$ y un único $D' \in \mathbb{Z}$ que no sea divisible por el cuadrado de ningún entero mayor que 1, es decir que o bien $D' = -1$ o bien $D' = \pm p_1 \dots p_t$ donde los $p_i$ son primos distintos de $\mathbb{Z}$. (Por ejemplo, $8/5 = (2/5)^2 \cdot 10$). Al entero $D'$ le llamamos *parte libre de cuadrados de* $D$. Entonces $\sqrt{D} = f\sqrt{D'}$ y por tanto $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$. Luego *no se pierde generalidad si se supone que* $D$ *es un entero libre de cuadrados en la definición del cuerpo cuadrático* $\mathbb{Q}[\sqrt{D}]$.

La aplicación $N : \mathbb{Q}[\sqrt{D}] \to \mathbb{Q}$ definida por $N(a + b\sqrt{D}) = (a + b\sqrt{D})\sigma(a + b\sqrt{D}) = a^2 - b^2D$ se llama *norma del cuerpo* $\mathbb{Q}[\sqrt{D}]$ (Por ejemplo, si $D < 0$ la norma $N(z)$ es sencillamente el cuadrado del módulo del número complejo $z$). La aplicación norma verifica las siguientes propiedades:

1. $N(uv) = N(u)N(v)$ para cualesquiera $u, v \in \mathbb{Q}[\sqrt{D}]$.
2. $N(u) = 0$ si y sólo si $u = 0$.

### 3.2.2. Anillos cuadráticos de enteros

Sea $D$ un entero libre de cuadrados. Es inmediato que el conjunto

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

es cerrado para la resta y el producto y contiene al número 1, luego es un subanillo del cuerpo cuadrático $\mathbb{Q}[\sqrt{D}]$.

En el caso en que $D \equiv 1 \pmod 4$, el conjunto ligeramente mayor

$$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] = \left\{c + b\frac{1+\sqrt{D}}{2} \mid c, b \in \mathbb{Z}\right\} = \left\{\frac{a + b\sqrt{D}}{2} \mid a, b \in \mathbb{Z},\ a \equiv b \pmod 2\right\}$$

también es un subanillo: Es inmediato que es cerrado para la resta y el 1 y el cálculo

$$(c + b\frac{1+\sqrt{D}}{2})(c_1 + b_1\frac{1+\sqrt{D}}{2}) = (cc_1 + bb_1\frac{D-1}{4}) + (cb_1 + c_1b + bb_1)\frac{1+\sqrt{D}}{2}$$

muestra que es cerrado para la multiplicación, ya que $(D-1)/4 \in \mathbb{Z}$.

Para unificar los dos casos, llamamos

$$\omega = \begin{cases} \sqrt{D} & \text{si } D \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & \text{si } D \equiv 1 \pmod 4 \end{cases}$$

y definimos

$$\mathcal{O} = \mathcal{O}_{\mathbb{Q}[\sqrt{D}]} = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

El anillo $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$ se llama *anillo de enteros del cuerpo cuadrático* $\mathbb{Q}[\sqrt{D}]$. La terminología proviene de que los elementos de $\mathcal{O}$ tienen muchas propiedades respecto a $\mathbb{Q}[\sqrt{D}]$ que son análogas a las de los enteros de $\mathbb{Z}$ respecto al cuerpo $\mathbb{Q}$ (En cursos posteriores se verá que $\mathcal{O}$ es la *clausura entera* de $\mathbb{Z}$ en $\mathbb{Q}[\sqrt{D}]$). La mas sencilla de estas propiedades es la siguiente:

**Lema 3.2.1.** *El cuerpo* $\mathbb{Q}[\sqrt{D}]$ *es el cuerpo de fracciones del dominio de integridad* $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$.

En el caso particular $D = -1$ obtenemos el anillo $\mathbb{J} = \mathbb{Z}[i]$ de los *enteros de Gauss*, que son los números complejos $a + bi \in \mathbb{C}$ con $a$ y $b$ enteros. Estos números fueron estudiados primero por Gauss alrededor del año 1800 para demostrar la *ley de reciprocidad bicuadrática*, que trata de las relaciones que existen entre las cuartas potencias módulo primos.

En los anillos $\mathcal{O}$ se utiliza la norma para caracterizar las unidades:

**Lema 3.2.2.** *Un elemento* $x = a + b\omega \in \mathcal{O}$ *es invertible en* $\mathcal{O}$ *si y sólo si* $N(x) = \pm 1$.

*Ejemplo* 3.2.3. Cuando $D = -1$, las unidades del anillo de enteros de Gauss son cuatro: $\pm 1, \pm i$ (que son las *raíces cuartas de la unidad*).

Cuando $D = -3$, las unidades del anillo $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ son los $a + b\omega$ tales que $a^2 + ab + b^2 = 1$, es decir los seis elementos $\pm 1, (\pm 1 \pm \sqrt{-3})/2$, que son las *raíces sextas de la unidad*.

Para cualquier otro $D < 0$, $D \neq -1, -3$, las unidades del anillo $\mathcal{O}$ son $1, -1$.

Cuando $D > 0$, se puede demostrar que el grupo de las unidades $\mathcal{O}^\times$ es siempre infinito. Por ejemplo, cuando $D = 2$ el grupo de las unidades es $\mathcal{O}^\times = \{\pm(1 + \sqrt{2})^k \mid k \in \mathbb{Z}\}$.

También utilizamos la norma para buscar irreducibles y primos en $\mathcal{O}$:

**Lema 3.2.4** (Condición suficiente de irreducibilidad)**.** *Sea* $u = a + b\sqrt{D}$ *tal que* $N(u) = \pm p$*, con* $p$ *primo en* $\mathbb{Z}$*. Entonces* $u$ *es irreducible*

*Demostración.* Sea $u = vw$. Entonces $N(v)N(w) = N(u) = \pm p$, así que o bien $N(v) = \pm 1$ (en cuyo caso $v$ es invertible) o bien $N(w) = \pm 1$ (en cuyo caso $w$ es invertible). □

**Lema 3.2.5** (Condición necesaria de primalidad)**.** *Sea* $u = a + b\sqrt{D}$ *primo en* $\mathcal{O}$*. Entonces* $N(u) = \pm p$ *o* $\pm p^2$ *con* $p$ *primo en* $\mathbb{Z}$*.*

*Si* $u$ *es primo en* $\mathcal{O}$*,* $u$ *es asociado con* $p$ *si y sólo si* $N(u) = \pm p^2$*.*

*Demostración.* Sabemos que $N(u) = u\sigma(u)$, así que $u$ divide al entero racional $N(u)$. Descomponemos en primos en $\mathbb{Z}$: $N(u) = p_1 \dots p_t$. Por ser $u$ primo debe dividir a uno de los factores $p = p_i$. Luego el entero racional $N(u)$ divide a $N(p) = p^2$. Como $N(u) \neq \pm 1$, sólo quedan las posibilidades del enunciado.

Sea $p = uv$. Se verifica que $p^2 = N(p) = N(u)N(v)$, así que $v$ es invertible si y sólo si $N(u) = \pm p^2$. □

**Corolario 3.2.6.** *Sea* $D < 0$, $D \neq -1, -3$*. Si* $u = a + b\omega$ *es primo y* $b \neq 0$*, necesariamente* $N(u) = p$ *es un primo en* $\mathbb{Z}$*.*

**Teorema 3.2.7.** *Sea* $D$ *un entero libre de cuadrados tal que* $\mathcal{O}$ *es un dominio de factorización única. Un elemento* $u \in \mathcal{O}$ *es primo si y sólo si es de uno de los siguientes tipos:*

- $u = \epsilon p$ *con* $\epsilon$ *invertible y* $p \in \mathbb{Z}$ *irreducible en* $\mathcal{O}$*.*
- $u = a + b\omega$ *con* $N(u) = \pm p$ *y* $p$ *primo en* $\mathbb{Z}$*.*

Podemos enunciar explícitamente los primos de un anillo cuadrático euclídeo:

**Teorema 3.2.8.** *Sea* $D$ *un entero libre de cuadrados tal que* $\mathcal{O}$ *es un dominio de factorización única.*

1. *Todo primo* $u$ *de* $\mathcal{O}$ *divide a un único primo* $p$ *de* $\mathbb{Z}$*.*
2. *Sea* $p$ *un primo de* $\mathbb{Z}$ *tal que* $p \nmid 2D$*.*
   a) $p = uv$ *es el producto de dos primos no asociados de* $\mathcal{O}$ *si y sólo si existe un* $a \in \mathbb{Z}$ *tal que* $a^2 \equiv D$ (mód $p$).

b) *$p$ es primo en $\mathcal{O}$ si y sólo si para todo $a \in \mathbb{Z}$ se verifica $a^2 \not\equiv D \pmod{p}$.*

3. a) *Sea $D \equiv 1 \pmod 8$. Entonces $2 = uv$ es el producto de dos primos no asociados de $\mathcal{O}$.*

   b) *Sea $D \equiv 5 \pmod 8$. Entonces 2 es primo en $\mathcal{O}$*

   c) *Sea $D \equiv 2, 3 \pmod 4$. Entonces $2 = \epsilon u^2$ es asociado al cuadrado de un primo de $\mathcal{O}$.*

4. *Sea $p \mid D$. Entonces $p = \epsilon u^2$ es asociado al cuadrado de un primo de $\mathcal{O}$.*

**Corolario 3.2.9.** *Sea $\mathbb{J} = \mathbb{Z}[i]$ el anillo de los enteros de Gauss y sea $p \in \mathbb{Z}$ un primo.*

1. *$p = (a + bi)(a - bi)$ es el producto de dos primos de $\mathbb{J}$ no asociados si y sólo si $p \equiv 1 \pmod 4$.*

2. *$p$ es primo en $\mathbb{J}$ si y sólo si $p \equiv 3 \pmod 4$.*

3. *El elemento $1 + i$ es primo en $\mathbb{J}$ y $2 = -i(1 + i)^2$.*

4. *Todo primo de $\mathbb{J}$ es de uno de los tipos anteriores.*

### 3.2.3. Anillos cuadráticos euclídeos

Los anillos $\mathcal{O}$ no son todos euclídeos, ni siquiera son dominios de factorización única. Pero vamos a ver que algunos de ellos son euclídeos respecto a la función $\phi : \mathcal{O} \to \mathbb{Z}$ definida por $\phi(u) = |N(u)|$ (valor absoluto de la norma).

En primer lugar, para cualquier par de elementos $u, v \in \mathcal{O}$ siempre se verifica que $\phi(uv) = \phi(u)\phi(v) \geq \phi(u)$ que es la primera condición de la definición de dominio euclídeo.

La segunda condición de dicha definición dice:

*Para $u, v \in \mathcal{O}$ con $v \neq 0$ existen $q, r \in \mathcal{O}$ tales que $u = vq + r$ y o bien $\phi(r) < \phi(v)$ o bien $r = 0$.*

Dividiendo por $v$ y teniendo en cuenta que $\mathbb{Q}[\sqrt{D}]$ es el cuerpo de fracciones de $\mathcal{O}$, esta condición se traduce en:

*Para todo $x \in \mathbb{Q}[\sqrt{D}]$ existe $q \in \mathcal{O}$ tal que o bien $|N(x - q)| < 1$ o bien $x = q$.*

Con esta condición podemos demostrar:

**Proposición 3.2.10.** *Sea $D = -2, -1$ o $2$. Entonces $\mathcal{O}$ es euclídeo respecto a la función $\phi$.*

*Demostración.* Nótese que los tres valores del enunciado son exactamente los $D$ libres de cuadrados con $|D| < 3$.

Sea $x = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$. Elegimos $q_1, q_2 \in \mathbb{Z}$ tales que $|a - q_1| \leq 1/2$ y $|b - q_2| \leq 1/2$ y llamamos $q = q_1 + q_2\sqrt{D}$. Entonces

$$\phi(x - q) = |N(x - q)| = |(a - q_1)^2 - (b - q_2)^2 D| \leq (a - q_1)^2 + (b - q_2)^2|D| < 1/4 + (1/4) \cdot 3 = 1$$

y por tanto $\mathbb{Q}[\sqrt{D}]$ es euclídeo.

Obsérvese que una vez conocido el cociente de dos elementos $u, v \in \mathcal{O}$, el resto se obtiene como $r = u - vq$. □

**Proposición 3.2.11.** *Sea $D = -11, -7, -3$ o $5$. Entonces $\mathcal{O}$ es euclídeo respecto a la función $\phi$.*

*Demostración.* Los valores del enunciado son exactamente los $D$ libres de cuadrados con $D \equiv 1 \pmod 4$ y $|D| < 12$.

Sea $x = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$. Elegimos $2q_1, 2q_2 \in \mathbb{Z}$ tales que $|b - q_2| \leq 1/4$, $2q_1 \equiv 2q_2 \pmod 2$ y $|a - q_1| \leq 1/2$ y llamamos $q = q_1 + q_2\sqrt{D}$. Entonces

$$\phi(x - q) = |N(x - q)| = |(a - q_1)^2 - (b - q_2)^2 D| \\ \leq (a - q_1)^2 + (b - q_2)^2|D| < 1/4 + (1/16) \cdot 12 = 1$$

y por tanto $\mathbb{Q}[\sqrt{D}]$ es euclídeo.

Como antes, una vez conocido el cociente de dos elementos $u, v \in \mathcal{O}$, el resto se obtiene como $r = u - vq$. □

Existen mas anillos cuadráticos euclídeos. En concreto la lista completa es la siguiente:

**Teorema 3.2.12.** *El anillo $\mathcal{O}$ es euclídeo respecto a la función $\phi$ anterior si y sólo si $D$ es uno de los valores*

$$-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

Esta lista no agota todos los anillos cuadráticos euclídeos, porque la función respecto a la que $\mathcal{O}$ es euclídeo no tiene porqué ser el valor absoluto de la norma. Se demuestra que para $D < 0$ el anillo $\mathcal{O}$ es euclídeo respecto a alguna función $\phi$ si y sólo si $D = -11, -7, -3, -2, -1$, pero es una conjetura que el conjunto de valores $D > 0$ para los que $\mathcal{O}$ es euclídeo es infinito. Por ejemplo para $D < 100$ el anillo $\mathcal{O}$, además de para los valores citados en el teorema anterior, también es euclídeo respecto a alguna función $\phi$ para los valores

$$D = 14, 22, 23, 31, 35, 38, 43, 46, 47, 53, 59, \\ 61, 62, 67, 69, 71, 77, 83, 86, 89, 93, 94, 97$$

Naturalmente para estos valores la función $\phi$ no es el valor absoluto de la norma.

## 3.3. Aritmética en dominios euclídeos

Los métodos y resultados que hemos estudiado para $\mathbb{Z}$ que se basan en el algoritmo de la división con resto se trasladan *mutatis mutande* a los anillos cuadráticos. En esta sección vamos a ver ejemplos de estos métodos en anillos cuadráticos euclídeos.

### 3.3.1. Factorización en primos

*Ejemplo* 3.3.1. Vamos a obtener la descomposición en primos de $u = 11 + 7i \in \mathbb{Z}[i]$:

En primer lugar calculamos y factorizamos en $\mathbb{Z}$ la norma de $u$:

$$N(u) = 11^2 + 7^2 = 121 + 49 = 170 = 2 \cdot 5 \cdot 17$$

Por el corolario 3.2.9, el elemento $u$ descompone como producto de un primo de norma 2, otro de norma 5 y un tercero de norma 17. Para cada uno de los valores 5 y 17 existen exactamente dos primos con dicha norma, y sólo hay un primo con norma 2. En total hay que probar como máximo cinco divisores. Empezamos sobre seguro, calculando el cociente de $u$ por el único primo (salvo asociados) de norma 2:

$$\frac{11 + 7i}{1 + i} = \frac{(11 + 7i)(1 - i)}{(1 + i)(1 - i)} = \frac{11 - 11i + 7i + 7}{2} = 9 - 2i$$

así que $u = (1+i)(9-2i)$. Probamos a dividir el cociente $9-2i$ por uno de los primos de norma 5:

$$\frac{9-2i}{2+i} = \frac{(9-2i)(2-i)}{(2+i)(2-i)} = \frac{18-9i-4i-2}{5} = \frac{16-11i}{5}$$

que no pertenece a $\mathbb{Z}[i]$. Luego $(2+i) \nmid (9-2i)$.

Probamos ahora con el otro primo de norma 5:

$$\frac{9-2i}{2-i} = \frac{(9-2i)(2+i)}{(2-i)(2+i)} = \frac{18+9i-4i+2}{5} = \frac{20+5i}{5} = 4+i$$

Este cociente pertenece a $\mathbb{Z}[i]$ y además es un primo de norma 17. Tenemos que $9-2i = (2-i)(4+i)$, luego la descomposición en primos del elemento dado es

$$11+7i = (1+i)(2-i)(4+i)$$

*Ejemplo* 3.3.2. Sea ahora $u = 4+7\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Su norma vale $N(u) = 4^2 - 7^2 2 = 16-98 = -2\cdot 41$, luego el elemento $u$ descompone como producto de un elemento de norma 2 y otro de norma 41, $u = \sqrt{2}(7+2\sqrt{2})$.

*Ejemplo* 3.3.3. Sea $u = 4-5\sqrt{-3} \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Calculamos la norma: $N(u) = 4^2 + 5^2 3 = 16+75 = 91 = 7\cdot 13$.

En $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ existen dos primos de norma 7 (que se obtienen resolviendo la ecuación $a^2+3b^2=7$), a saber $2+\sqrt{-3}$ y $2-\sqrt{-3}$. Probamos a dividir por el primero:

$$\frac{4-5\sqrt{-3}}{2+\sqrt{-3}} = \frac{(4-5\sqrt{-3})(2-\sqrt{-3})}{(2+\sqrt{-3})(2-\sqrt{-3})} = \frac{8-4\sqrt{-3}-10\sqrt{-3}-15}{7}$$

$$= \frac{-7-14\sqrt{-3}}{7} = -1-2\sqrt{-3}$$

así que la factorización en primos es

$$4-5\sqrt{-3} = (2+\sqrt{-3})(-1-2\sqrt{-3})$$

### 3.3.2. Cálculo del máximo común divisor

Igual que en $\mathbb{Z}$, en cualquier anillo euclídeo tenemos dos métodos para calcular el máximo común divisor: Uno es factorizar en primos cada elemento dado y formar "el producto de los factores comunes elevados al menor exponente":

*Ejemplo* 3.3.4. Sean $a = 1+3i$, $b = 3+4i$ dos elementos de $\mathbb{Z}[i]$. Buscamos sus respectivas factorizaciones en primos:

$$N(a) = 1^2+3^2 = 10 = 2\cdot 5, \qquad \frac{1+3i}{1+i} = \frac{(1+3i)(1-i)}{(1+i)(1-i)} = 2+i$$

$$N(b) = 3^2+4^2 = 25 = 5^2, \qquad \frac{3+4i}{2+i} = \frac{(3+4i)(2-i)}{(2+i)(2-i)} = 2+i$$

así que $a = (1+i)(2+i)$, $b = (2+i)^2$, $\text{m.c.d.}(a,b) = 2+i$ y $\text{m.c.m.}(a,b) = (1+i)(2+i)^2 = -1+7i$

El otro método es aplicar el algoritmo de Euclides (simple o extendido). El máximo común divisor será el último resto no nulo.

*Ejemplo* 3.3.5. Sean $a = 11 + 7i$, $b = 3 + 7i$ dos elementos de $\mathbb{Z}[i]$. Calculamos

$$\frac{11+7i}{3+7i} = \frac{(11+7i)(3-7i)}{(3+7i)(3-7i)} = \frac{82}{58} - \frac{56}{58}i$$

así que tomamos el cociente $q_1 = 1 - i$ y el resto $r_1 = a - bq_1 = 1 + 3i$. Dividimos ahora $b$ por $r_1$:

$$\frac{3+7i}{1+3i} = \frac{(3+7i)(1-3i)}{(1+3i)(1-3i)} = \frac{24}{10} - \frac{2}{10}i$$

El nuevo cociente será $q_2 = 2$ y el resto $r_2 = b - r_1q_2 = 1 + i$. El siguiente paso es dividir $r_1$ por $r_2$:

$$\frac{1+3i}{1+i} = \frac{(1+3i)(1-i)}{(1+i)(1-i)} = 2 + i$$

con lo que $q_3 = 2 + i$ y $r_3 = 0$. Luego m. c. d.$(a, b) = 1 + i$ (el último resto no nulo).

Para obtener los coeficientes de Bezout utilizamos el algoritmo extendido de Euclides:

| $q$ | | $u$ | $v$ |
|---|---|---|---|
| | $11 + 7i$ | $1$ | $0$ |
| | $3 + 7i$ | $0$ | $1$ |
| $1 - i$ | $1 + 3i$ | $1$ | $-1 + i$ |
| $2$ | $1 + i$ | $-2$ | $3 - 2i$ |
| $2 + i$ | $0$ | | |

así que $(11 + 7i)(-2) + (3 + i)(3 - 2i) = 1 + i$.

*Ejemplo* 3.3.6. Vamos a calcular ahora el máximo común divisor de $a = (5 + \sqrt{-11})/2$ y $b = 2 + \sqrt{-11}$ en el anillo $A = \mathbb{Z}[(1 + \sqrt{-11})/2]$. Como $N(a) = (5^2 + 11)/4 = 9$ y $N(b) = 2^2 + 11 = 15$, empezamos dividiendo $b$ entre $a$:

$$\frac{2+\sqrt{-11}}{(5+\sqrt{-11})/2} = \frac{2(2+\sqrt{-11})(5-\sqrt{-11})}{(5+\sqrt{-11})(5-\sqrt{-11})} = \frac{2(21+3\sqrt{-11})}{36} = \frac{7+\sqrt{-11}}{6}$$

así que el cociente es $q = 1$ y el resto $r = b - aq = (-1 + \sqrt{-11})/2$. Dividimos ahora $a$ entre $r$:

$$\frac{(5+\sqrt{-11})/2}{(-1+\sqrt{-11})/2} = \frac{(5+\sqrt{-11})(-1-\sqrt{-11})}{(-1+\sqrt{-11})(-1-\sqrt{-11})} = \frac{6-6\sqrt{-11}}{12} = \frac{1-\sqrt{-11}}{2}$$

que pertenece a $\mathbb{Z}[(1 + \sqrt{-11})/2]$, así que $q_1 = (1 - \sqrt{-11})/2$ y $r_1 = 0$. Vamos a calcular los coeficientes de Bezout:

| $q$ | | $u$ | $v$ |
|---|---|---|---|
| | $2 + \sqrt{-11}$ | $1$ | $0$ |
| | $\frac{5+\sqrt{-11}}{2}$ | $0$ | $1$ |
| $1$ | $\frac{-1+\sqrt{-11}}{2}$ | $1$ | $-1$ |
| $\frac{1-\sqrt{-11}}{2}$ | $0$ | | |

luego m. c. d.$(a, b) = \frac{-1+\sqrt{-11}}{2} = b \cdot 1 + a \cdot (-1)$

### 3.3.3. Resolución de ecuaciones lineales

En nuestra exposición de $\mathbb{Z}$ vimos cómo utilizar el algoritmo extendido de Euclides para resolver ecuaciones diofánticas lineales en dos incógnitas. Exactamente el mismo método se aplica para resolver ecuaciones lineales en anillos euclídeos. En concreto tenemos el siguiente teorema:

Sea $A$ un anillo euclídeo y sean $a, b, c \in A$. Consideramos la ecuación

$$ax + by = c \tag{3.3.1}$$

**Teorema 3.3.7.** *1. La ecuación 3.3.1 tiene solución si y sólo si* $\text{m. c. d.}(a, b) \mid c$.

*2. Una solución particular de 3.3.1 se obtiene por el algoritmo extendido de Euclides.*

*3. Sea* $d = \text{m. c. d.}(a, b)$ *y sea* $(x_0, y_0)$ *una solución particular de 3.3.1. La solución general* $(x, y)$ *viene dada por*

$$x = x_0 + k\frac{b}{d}, \qquad y = y_0 - k\frac{a}{d}$$

*con* $k \in A$ *arbitrario.*

*Demostración.* La demostración es idéntica a la realizada en el caso $A = \mathbb{Z}$, que se basaba sólo en la existencia del algoritmo de división con resto. □

*Ejemplo* 3.3.8. Consideramos la ecuación siguiente en $\mathbb{Z}[i]$:

$$4x + (3 + 3i)y = -1 + 5i$$

Para discutirla y en su caso resolverla, calculamos el máximo común divisor de los coeficientes:

| $q$ | | $u$ | $v$ |
|---|---|---|---|
| | $3+3i$ | 1 | 0 |
| | 4 | 0 | 1 |
| $1+i$ | $-1-i$ | 1 | $-1-i$ |
| $-2+2i$ | 0 | | |

luego el máximo común divisor es $-1-i = (3+3i)-4\cdot(1+i)$. Calculamos el cociente $(-1+5i)/(-1-i) = -2-3i$ que pertenece a $\mathbb{Z}[i]$, luego la ecuación dada tiene solución. Una solución particular será

$$x_0 = -(1 + i)(-2 - 3i) = -1 + 5i, \qquad y_0 = -2 - 3i$$

y la solución general es

$$\begin{aligned} x &= -1 + 5i + k \cdot 3 \\ y &= -2 - 3i - k \cdot (2 - 2i) \end{aligned}$$

con $k \in \mathbb{Z}[i]$ arbitrario.

### 3.3.4. Resolución de ecuaciones en congruencias

También podemos establecer en cualquier anillo euclídeo el concepto de congruencia módulo un elemento:

**Definición 3.3.9.** Sea $A$ un anillo euclídeo y sea $m \in A$. Los elementos $a, b \in A$ se llaman *congruentes módulo* $m$ si tienen el mismo resto al dividirlos por $m$. Esto se denota por $a \equiv b \pmod{m}$ o $a \equiv b \mod m$

**Proposición 3.3.10.** *Sean $a, b, m \in A$. Entonces $a \equiv b \pmod{m}$ si y sólo si $m \mid (a - b)$.*

Esta proposición nos dice que $a \equiv b \pmod{m}$ si y sólo si $a - b = mq$ para algún $q \in A$, lo que podemos escribir como $a = b + mq$. Esta observación proporciona un método muy útil de reemplazar una congruencia por una ecuación diofántica.

**Proposición 3.3.11.** *La relación $a \equiv b \pmod{m}$ es una relación de equivalencia.*

**Proposición 3.3.12.** *Sea $m \in A$. Cualesquiera $a, b, c, d \in A$ verifican las siguientes propiedades:*

1. *Si $a \equiv c \pmod{m}$ y $b \equiv d \pmod{m}$, entonces $a + b \equiv c + d \pmod{m}$, $a - b \equiv c - d \pmod{m}$ y $ab \equiv cd \pmod{m}$.*
2. *Si $a + c \equiv a + d \pmod{m}$ entonces $c \equiv d \pmod{m}$. Si $ac \equiv ad \pmod{m}$ y $(a, m) = 1$ entonces $c \equiv d \pmod{m}$.*

**Proposición 3.3.13.** *Sean $a, m \in A$ con $m \neq 0$ y no invertible en $A$. Existe un elemento $b$ tal que $ab \equiv 1 \pmod{m}$ si y sólo si $\text{m. c. d.}(a, m) = 1$.*

La proposición 3.3.13 muestra que la congruencia

$$ax \equiv 1 \pmod{m}$$

tiene solución si y sólo si $(a, m) = 1$. De hecho la demostración (omitida) de dicha proposición muestra que se obtiene una solución utilizando el algoritmo extendido de Euclides para expresar $1 = ab + mq$ con $b, q \in A$.

**Definición 3.3.14.** Dos soluciones $r$ y $s$ a la congruencia $ax \equiv b \pmod{m}$ son distintas módulo $m$ si $r$ y $s$ no son congruentes módulo $m$.

**Teorema 3.3.15.** *La congruencia $ax \equiv b \pmod{m}$ tiene solución si y sólo si $b$ es divisible por $d = \text{m. c. d.}(a, m)$. Si $d \mid b$, todas las soluciones son congruentes módulo $m/d$.*

*Ejemplo* 3.3.16. Consideramos $A = \mathbb{Z}[\sqrt{2}]$. Vamos a resolver la congruencia

$$(2 + \sqrt{2})x \equiv 3 - \sqrt{2} \pmod{3}$$

Para ello calculamos el máximo común divisor de $2 + \sqrt{2}$ y 3:

| $q$ | $u$ | $v$ |
|---|---|---|
| | 3 | 1 | 0 |
| | $2 + \sqrt{2}$ | 0 | 1 |
| $3 - \sqrt{2}$ | $-1 - \sqrt{2}$ | 1 | $-3 + \sqrt{2}$ |
| $-\sqrt{2}$ | 0 | | |

así que un máximo común divisor es $-1 - \sqrt{2} = 3 \cdot 1 + (2 + \sqrt{2}) \cdot (-3 + \sqrt{2})$. Ahora $(3 - \sqrt{2})/(-1 - \sqrt{2}) = 5 - 4\sqrt{2}$, luego la solución de la congruencia dada es $x \equiv (-3 + \sqrt{2})(5 - 4\sqrt{2}) \equiv -23 + 17\sqrt{2} \equiv 1 - \sqrt{2} \pmod{3}$. Obsérvese que $-1 - \sqrt{2}$ es invertible en $\mathbb{Z}[\sqrt{2}]$ (su inverso es $1 - \sqrt{2}$), así que $2 + \sqrt{2}$ y 3 son primos relativos y la solución es única módulo 3.

**Teorema 3.3.17.** *Sea $A$ un dominio euclídeo y sean $a, b, m, n \in A$. Dos congruencias simultáneas*

$$x \equiv a \pmod{m} \qquad x \equiv b \pmod{n} \tag{3.3.2}$$

*tienen solución si y sólo si $a \equiv b \pmod{(m, n)}$. En este caso la solución es única módulo $[m, n]$.*

*Ejemplo* 3.3.18. Vamos a resolver en $A = \mathbb{Z}[\sqrt{-2}]$ el sistema de congruencias

$$\begin{aligned} x &\equiv 2 \pmod{(1+\sqrt{-2})} \\ x &\equiv \sqrt{-2} \pmod{(3+\sqrt{-2})} \end{aligned}$$

La solución general de la primera congruencia es $x = 2 + t_1 \cdot (1+\sqrt{-2})$. Lo sustituimos en la segunda:

$$2 + t_1 \cdot (1+\sqrt{-2}) \equiv \sqrt{-2} \pmod{(3+\sqrt{-2})}$$

Trasponiendo términos nos queda

$$t_1 \cdot (1+\sqrt{-2}) \equiv -2 + \sqrt{-2} \pmod{(3+\sqrt{-2})} \tag{3.3.3}$$

Aplicamos ahora el algoritmo de Euclides extendido:

| $q$ | $u$ | $v$ |
|---|---|---|
| | $3+\sqrt{-2}$ | $1$ | $0$ |
| | $1+\sqrt{-2}$ | $0$ | $1$ |
| $2-\sqrt{-2}$ | $-1$ | $1$ | $-2+\sqrt{-2}$ |

así que $(3+\sqrt{-2})\cdot 1 + (1+\sqrt{-2})(-2+\sqrt{-2}) = -1$. Luego la solución de 3.3.3 es $t_1 = (-2+\sqrt{-2})(2-\sqrt{-2}) + u\cdot(3+\sqrt{-2}) = -2 + 4\sqrt{-2} + t\cdot(3+\sqrt{-2})$. Sustituyendo en la primera solución obtenemos la solución general del sistema:

$$\begin{aligned} x &= 2 + (1+\sqrt{-2})(-2 + 4\sqrt{-2} + t\cdot(3+\sqrt{-2})) \\ &= -8 + 2\sqrt{-2} + t\cdot(1+4\sqrt{-2}) \end{aligned}$$

*Ejemplo* 3.3.19. Vamos ahora a resolver el sistema

$$\begin{aligned} x &\equiv 1 + 2\sqrt{-2} \pmod{(2-3\sqrt{-2})} \\ x &\equiv 3 \pmod{(1+\sqrt{-2})} \end{aligned}$$

Desarrollamos el algoritmo extendido de Euclides:

| $q$ | $u$ | $v$ |
|---|---|---|
| | $2-3\sqrt{-2}$ | $1$ | $0$ |
| | $1+\sqrt{-2}$ | $0$ | $1$ |
| $-1-2\sqrt{-2}$ | $-1$ | $1$ | $1+2\sqrt{-2}$ |

así que $(2-3\sqrt{-2})\cdot 1 + (1+\sqrt{-2})(1+2\sqrt{-2}) = -1$ y los módulos de las congruencias son primos relativos. Luego el sistema de ecuaciones tiene solución.

La solución general de la primera ecuación es

$$x = (1+\sqrt{-2}) + (2-3\sqrt{-2})t_1$$

Sustituyendo en la segunda y trasponiendo términos nos queda la ecuación

$$(2-3\sqrt{-2})t_1 \equiv 3 - (1+2\sqrt{-2}) = 2 - 2\sqrt{-2} \pmod{(1+\sqrt{-2})}$$

Por el algoritmo de Euclides calculado tenemos que

$$t_1 \equiv -1 \cdot (2 - 2\sqrt{-2}) = -2 + 2\sqrt{-2} \pmod{(1 + \sqrt{-2})}$$

Sustituyendo en la solución de la primera obtenemos la solución general del sistema:

$$\begin{aligned} x &= (1 + \sqrt{-2}) + (2 - 3\sqrt{-2})((-2 + 2\sqrt{-2}) + (1 + \sqrt{-2})t) \\ &= (9 + 11\sqrt{-2}) + (8 - \sqrt{-2})t \end{aligned}$$

**Teorema 3.3.20.** *Sea $A$ un dominio euclídeo y sean $a_i, m_i \in A$ para $i = 1, \ldots, r$. Un sistema de $r$ congruencias simultáneas*

$$x \equiv a_i \pmod{m_i} \quad i = 1, 2, \ldots, r \tag{3.3.4}$$

*tiene solución si y sólo si para todo par de índices $i, j$ se verifica*

$$a_i \equiv a_j \pmod{(m_i, m_j)} \tag{3.3.5}$$

*y en este caso la solución es única módulo $M_r = [m_1, \ldots, m_r]$.*

*Ejemplo* 3.3.21. Vamos a tomar$A = \mathbb{Z}[i]$, el anillo de los enteros de Gauss y consideramos el sistema de congruencias:

$$\begin{aligned} x &\equiv i \pmod{3} \\ x &\equiv 2 \pmod{(2 + i)} \\ x &\equiv 1 + i \pmod{(3 + 2i)} \\ x &\equiv 3 + 2i \pmod{(4 + i)} \end{aligned}$$

El máximo común divisor de los dos primeros módulos es $3 \cdot (-i) + (2 + i)(1 + i) = 1$. La solución general de la primera ecuación es

$$x = i + 3t_1$$

Sustituyendo en la segunda ecuación nos queda $3t_1 \equiv 2 - i \pmod{(2 + i)}$. Luego $t_1 \equiv -i \cdot (2 - i) = -1 - 2i \pmod{(2 + i)}$ y la solución general de las dos primeras ecuaciones es

$$\begin{aligned} x &= i + 3(-1 - 2i + (2 + i)t_2 \\ &= -3 - 5i + (6 + 3i)t_2 \end{aligned}$$

Sustituimos en la tercera ecuación y despejamos: $(6 + 3i)t_2 \equiv 4 + 6i \pmod{(3 + 2i)}$. El algoritmo extendido de Euclides muestra que $(6 + 3i)i + (3 + 2i)(-2i) = 1$ por lo que $t_2 \equiv i(4 + 6i) \pmod{(3 + 2i)}$. La solución general de las tres primeras ecuaciones es ahora

$$\begin{aligned} x &= -3 - 5i + (6 + 3i)(i(4 + 6i) + (3 + 2i)t_3) \\ &= -51 + i + (12 + 21i)t_3 \end{aligned}$$

Finalmente sustituimos este valor en la cuarta ecuación y despejamos:

$$(12 + 21i)t_3 \equiv 54 + i \pmod{(4 + i)}$$

La aplicación correspondiente del algoritmo de Euclides nos da $(-i)(12 + 21i) + (-4 + 4i)(4 + i) = 1$. Luego $t_3 \equiv (-i)(54 + i) = 1 - 54i \pmod{(4 + i)}$ y la solución general del sistema dado es

$$\begin{aligned} x &= -51 + i + (12 + 21i)((1 - 54i) + (4 + i)t) \\ &= 1095 - 626i + (27 + 96i)t \\ &= 24 - 14i + (27 + 96i)t \end{aligned}$$

donde la última reducción se obtiene por el cambio $t \to t + (3 + 12i)$. (El algoritmo de división nos da $1095 - 626i = (27 + 96i)(-3 - 12i) + (24 - 14i)$).

*Ejemplo* 3.3.22. Cuando los módulos de un sistema de congruencias son primos relativos dos a dos, podemos emplear el algoritmo chino del resto. Volvamos a resolver el sistema del ejemplo anterior:

$$\begin{aligned} x &\equiv i \pmod 3 \\ x &\equiv 2 \pmod{(2+i)} \\ x &\equiv 1+i \pmod{(3+2i)} \\ x &\equiv 3+2i \pmod{(4+i)} \end{aligned}$$

Formamos el producto de todos los módulos $M = 3(2+i)(3+2i)(4+i) = 27+96i$ y cada uno de los cocientes $M_1 = M/3 = 9+32i$, $M_2 = M/(2+i) = 30+33i$, $M_3 = M/(3+2i) = 21+18i$ y $M_4 = M/(4+i) = 12+21i$. El algoritmo de Euclides para cada uno de los cuatro casos nos da

$$\begin{aligned} i(9+32i) + (11-3i)3 &= 1 \\ (-1)(30+33i) + (19+7i)(2+i) &= 1 \\ 2(21+18i) + (-15-2i)(3+2i) &= 1 \\ (-i)(12+21i) + (-4+4i)(4+i) &= 1 \end{aligned}$$

El teorema chino del resto nos dice que la solución del sistema dado es

$$\begin{aligned} x &\equiv i \cdot i(9+32i) + 2 \cdot (-1)(30+33i) \\ &\quad + (1+i) \cdot 2(21+18i) + (3+2i) \cdot (-i)(12+21i) \\ &\equiv 24-14i \pmod{(27+96i)} \end{aligned}$$

## 3.4. Ejercicios

**Ejercicio 3.1.** Demostrar que en un anillo la conmutatividad de la suma es consecuencia de los restantes axiomas.

**Ejercicio 3.2.** Sea $X$ un conjunto no vacío y $R = P(X)$, el conjunto de partes de $X$. Si se consideran en $R$ las operaciones:

$$A + B = (A \cap \overline{B}) \cup (\overline{A} \cap B)$$

$$A \times B = A \cap B$$

demostrar que $(R, +, \times)$ es un anillo con elemento 1 igual a $X$.

**Ejercicio 3.3.** Sea $A$ un grupo abeliano y consideremos el producto cartesiano $R = \mathbb{Z} \times A$. Si en $R$ definimos las siguientes operaciones:

$$(n, a) + (m, b) = (n + m, a + b)$$

$$(n, a)(m, b) = (nm, ma + nb)$$

demostrar que $(R, +, .)$ es un anillo conmutativo con elemento 1 igual a (1,0).

**Ejercicio 3.4.** En el conjunto $\mathbb{Z}$ de los enteros se definen las siguientes operaciones:

$$a \oplus b = a + b - 1 \text{ y } a \otimes b = a + b - ab.$$

Demuestra que $\langle \mathbb{Z}, \oplus, \otimes \rangle$ es un dominio de integridad.

**Ejercicio 3.5.** En el conjunto $\mathbb{Z} \times \mathbb{Z}$ de las parejas de enteros se definen las siguientes operaciones:

$$(a, b) + (c, d) = (a + c, b + d) \text{ y } (a, b)(c, d) = (ac, bd)$$

Demuestra que $\langle \mathbb{Z} \times \mathbb{Z}, +, . \rangle$ es un anillo conmutativo. Prueba que no es dominio de integridad y calcula sus unidades y sus divisores de cero.

**Ejercicio 3.6.** En una anillo R un elemento es idempotente si $a^2 = a$. Demuestra que en un anillo íntegro (sin divisores de cero) los únicos idempotentes son 0 y 1.

**Ejercicio 3.7.** Dados dos elementos a y b de un anillo R. Demuestra que si $1 - ab$ es una unidad entonces $1 - ba$ también lo es.

**Ejercicio 3.8.** Sea R un anillo conmutativo y $a \in R$. Demuestra que las siguientes afirmaciones son equivalentes:

1. a es un divisor de cero.
2. Existe $b \in R$ no nulo tal que $aba = 0$.

**Ejercicio 3.9.** Sean a y b elementos de un anillo $R$ tales que $a, b$ y $ab - 1$ son unidades. Demuestra que $a - b^{-1}$ y $(a - b^{-1})^{-1} - a^{-1}$ también lo son y que se verifica la igualdad $((a - b^{-1})^{-1} - a^{-1})^{-1} = aba - a$.

**Ejercicio 3.10.** Determinar los ideales del anillo cociente $\mathbb{Z}/n\mathbb{Z}$. Describir el retículo de ideales de este anillo cuando $n = pq$ siendo $p$ y $q$ primos positivos distintos.

**Ejercicio 3.11.** Calcular los divisores de cero en el anillo $\mathbb{Z}/n\mathbb{Z}$.

**Ejercicio 3.12.** Sea $X$ el conjunto de los elementos no nulos del anillo $\mathbb{Z}/10\mathbb{Z}$. En $X$ se define la siguiente relación de equivalencia:

$$x\,R\,y \;\Leftrightarrow x \mid y \;\wedge\; y \mid x$$

Describir el conjunto cociente $X/R$ determinando cuantas clases de equivalencia hay y que elementos hay en cada clase.

**Ejercicio 3.13.** Calcula $\mathcal{U}(M_2(\mathbb{Z}))$ las unidades del anillo $M_2(\mathbb{Z})$ de las matrices $2 \times 2$ con coeficientes enteros.

**Ejercicio 3.14.** Demuestra que todo anillo de división es un anillo íntegro y por tanto todo cuerpo es un dominio de integridad.

**Ejercicio 3.15.** Sea $R$ un dominio de integridad y $a, b, c \in R$. Demostrar:

1. $b|a \Rightarrow b|ac$.
2. $\left.\begin{array}{l} b|a \\ c|b \end{array}\right\} \Rightarrow c|a.$
3. $\left.\begin{array}{l} b|a \\ b|(a+c) \end{array}\right\} \Rightarrow b|c.$
4. $\left.\begin{array}{l} b|a \\ b \nmid c \end{array}\right\} \Rightarrow b \nmid (a+c).$
5. Si $c \neq 0$, $bc|ac \Leftrightarrow b|a$.

**Ejercicio 3.16.** Sea $A$ el subconjunto de $M_2(\mathbb{C})$ dado por

$$A = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : \; a, b \in \mathbb{C} \right\}$$

¿Es $A$ un anillo de división? Halla el inverso de cada uno de los elementos:

$$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

**Ejercicio 3.17.** Sea $A$ el subconjunto de $M_2(\mathbb{C})$ dado por

$$A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : \; a, b \in \mathbb{R} \right\}$$

demuestra que es un cuerpo.

**Ejercicio 3.18.** Sea $A$ el subconjunto de $M_2(\mathbb{Z})$ dado por

$$A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : \; a, b \in \mathbb{Z} \right\}$$

demuestra que es un dominio de integridad. Halla sus unidades.

**Ejercicio 3.19.** Sea $d \in \mathbb{Z}$ un entero y $A_d$ el subconjunto de $M_2(\mathbb{Z})$ dado por

$$A_d = \left\{ \begin{pmatrix} a & b \\ bd & a \end{pmatrix} : \ a, b \in \mathbb{Z} \right\}$$

Encontrar los enteros $d$ para los cuales $A_d$ es un dominio de integridad. Halla sus unidades en el caso de que $d \in \mathbb{Z}^-$.

**Ejercicio 3.20.** Sabiendo que $sa + tb = 1$, prueba o da un contraejemplo de las siguientes afirmaciones:

$$\text{a) } (sa, tb) = 1 \ , \qquad \text{b) } (sb, ta) = 1 \ , \qquad \text{c) } (st, ab) = 1.$$

**Ejercicio 3.21.** Estudia que tipo de anillos son $\mathbb{Z}_7$ y $\mathbb{Z}_9$. Halla sus unidades y sus divisores de cero.

**Ejercicio 3.22.** Si $n$ es impar, prueba que $\bar{2} \in \mathcal{U}(\mathbb{Z}_n)$.

**Ejercicio 3.23.** El conjunto $A = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\} \subseteq \mathbb{Z}/10\mathbb{Z}$ es cerrado para la suma y el producto.

- Demostrar que $A$ es un cuerpo.
- Demostrar que $A$ no es un subanillo de $\mathbb{Z}/10\mathbb{Z}$.

**Ejercicio 3.24.** ¿Cuales de los siguientes conjuntos son subanillos del cuerpo $\mathbb{Q}$ de los números racionales?

1. $\{\frac{n}{m} \mid m \text{ es impar}\}$
2. $\{\frac{n}{m} \mid m \text{ es par}\}$
3. $\{\frac{n}{m} \mid 4 \nmid m\}$
4. $\{\frac{n}{m} \mid (m, 6) = 1\}$
5. +Es alguno de los subconjuntos anteriores un ideal de $\mathbb{Q}$?

Nota: Siempre que aparece $\frac{n}{m}$ estamos suponiendo que $(n, m) = 1$.

**Ejercicio 3.25.** Dado un anillo $A$, el conjunto $A \times A$ es de nuevo un anillo. ¿Es el subconjunto

$$\{(a, 2a) \mid a \in A\} \subseteq A \times A$$

un ideal o un subanillo de $A \times A$? (Razona la respuesta dada.)

**Ejercicio 3.26.** Sea $f : R \to R$ un homomorfismo de anillos y sea $S = \{a \in R / f(a) = a\}$. Demostrar que $S$ es un subanillo de $R$.

**Ejercicio 3.27.** Sea $R$ un anillo y sea $a \in R$ un elemento invertible. Demostrar que la aplicación $f_a : R \to R$ dada por $f_a(x) = axa^{-1}$ es un automorfismo de $R$.

**Ejercicio 3.28.** Dado un anillo $R$, demostrar que existe un único homomorfismo de anillos de $\mathbb{Z}$ en $R$.

**Ejercicio 3.29.** Demostrar que si $A$ es un anillo de característica $n$ entonces existe un único homomorfismo de anillos de $\mathbb{Z}/n\mathbb{Z}$ en $A$ y que además este homomorfismo es inyectivo.

**Ejercicio 3.30.** Dados dos números naturales $n$ y $m$, dar condiciones para que exista un homomorfismo de anillos de $\mathbb{Z}/n\mathbb{Z}$ en $\mathbb{Z}/m\mathbb{Z}$.

**Ejercicio 3.31.** Describir los ideales de $\mathbb{Z}/14\mathbb{Z}$ enumerando los elementos de cada uno de ellos.

**Ejercicio 3.32.** Si $A$ y $B$ son dos anillos conmutativos demostrar que todos los ideales del anillo producto $A \times B$ son de la forma $\alpha \times \beta$ donde $\alpha$ es un ideal de $A$ y $\beta$ es un ideal de $B$.

**Ejercicio 3.33.** Razonar si las siguientes afirmaciones son verdaderas o falsas:

i) El anillo $\frac{\mathbb{Z}}{(6\mathbb{Z}+4\mathbb{Z})\cap 5\mathbb{Z}} \times \mathbb{Q}$ tiene 4 unidades, 8 ideales e infinitos divisores de cero.

ii) Existe un único homomorfismo de anillos de $\mathbb{Z}$ en $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{7\mathbb{Z}}$ que es sobreyectivo.

iii)$\mathbb{Z}_{1457}$ es un cuerpo.

iv) De $\mathbb{Z}_7$ en $\mathbb{Z}_{14}$ hay exactamente 7 homomorfismos de anillos.

**Ejercicio 3.34.** Sea $D$ un DFU y $a, b \in D$. Si $ab \neq 0$ y $d \in D$ es un divisor de $ab$ que es primo relativo con $a$ probar que entonces $d$ divide a $b$.

**Ejercicio 3.35.** Sea $D$ un DFU y $a, b \in D$ no nulos. Si $d = m.c.d.(a, b)$ y $a = da'$, $b = db'$, demostrar que $a'$ y $b'$ son primos relativos.

**Ejercicio 3.36.** Calcular en $\mathbb{Z}[i]$ todos los elementos $z$ que cumplan $N(z) \leq 5$, ¿cuales de ellos son irreducibles?.

**Ejercicio 3.37.** Calcula $\mathcal{U}(R)$ las unidades del anillo $R$ en los casos $R = \mathbb{Z}[i]$ y $R = \mathbb{Z}[\sqrt{-5}]$.

**Ejercicio 3.38.** Comprobar que los elementos $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$ son irreducibles en $\mathbb{Z}[\sqrt{10}]$ pero no son primos. Como consecuencia deducir que $\mathbb{Z}[\sqrt{10}]$ no es un DFU encontrando dos factorizaciones de 6 distintas.

**Ejercicio 3.39.** Demostrar que los elementos $2, 7, 1 + \sqrt{-13}$ y $1 - \sqrt{-13}$ son irreducibles no asociados en $\mathbb{Z}[\sqrt{-13}]$. Encontrar dos factorizaciones distintas en irreducibles de 14 y a partir de ella concluir que en $\mathbb{Z}[\sqrt{-13}]$ hay elementos irreducibles que no son primos. ¿Es $\mathbb{Z}[\sqrt{-13}]$ un dominio euclídeo?.

**Ejercicio 3.40.** En el anillo $\mathbb{Z}[i]$ calcular el máximo común divisor y el mínimo común múltiplo de $a = 2i$ y $b = 3 - 7i$. Calcular además elementos $u$ y $v$ tales que $ua + vb = \text{mcd}(a, b)$.

**Ejercicio 3.41.** Calcular las unidades de $\mathbb{Z}[\sqrt{-3}]$ y demostrar que este anillo no es un DFU viendo que $4 = 2{,}2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ son dos factorizaciones en irreducibles distintas del elemento 4. Razonar que los elementos en las factorizaciones no son primos.

**Ejercicio 3.42.** En el anillo $\mathbb{Z}[i]$ calcular elementos $u$ y $v$ tales que

$$(2 + 5i)u + (3 - 4i)v = 1 + i.$$

**Ejercicio 3.43.** Da la solución general, si existe, de la ecuación diofántica en $\mathbb{Z}[i]$,

$$4x + (3 + 3i)y = -1 + 5i\ .$$

**Ejercicio 3.44.** Factoriza $15 + 42i$ y $9 - 2i$ en $\mathbb{Z}[i]$. Calcula m. c. d.$(15 + 42i, 9 - 2i)$.

**Ejercicio 3.45.** En $\mathbb{Z}[\sqrt{3}]$ factoriza $3 + \sqrt{3}$ en irreducibles y calcula m. c. d.$(3 + \sqrt{3}, 2)$ y m. c. m.$(3 + \sqrt{3}, 2)$.

**Ejercicio 3.46.** Demuestra que los elementos $2, 1 + \sqrt{-7}, 1 - \sqrt{-7}$ de $\mathbb{Z}[\sqrt{-7}]$ son irreducibles pero no son primos y encuentra dos factorizaciones que no sean esencialmente idénticas de 8 en irreducibles. ¿Que se puede concluir entonces de las propiedades aritméticas de $\mathbb{Z}[\sqrt{-7}]$?

**Ejercicio 3.47.** Sea $a + bi \in \mathbb{Z}[i]$ un elemento tal que $ab \neq 0$. Probar que es primo si y solo si $a^2 + b^2$ es un primo.

**Ejercicio 3.48.** En el anillo $\mathbb{Z}[i]$ se consideran los elementos $x = 1 + 3i$, $y = 3 + 4i$. Factorizar $x$ e $y$ como producto de irreducibles y calcular su m.c.d. y su m.c.m.

**Ejercicio 3.49.** En el anillo $\mathbb{Z}[i]$ resolver el siguiente sistema de congruencias

$$\left.\begin{array}{rcccc} x & \equiv & i & \mod & 3 \\ x & \equiv & 2 & \mod & 2+i \\ x & \equiv & 1+i & \mod & 3+2i \\ x & \equiv & 3+2i & \mod & 4+i \end{array}\right\}$$

**Ejercicio 3.50.** Resolver, dando la solución general, el siguiente sistema de congruencias en $\mathbb{Z}[i]$:

$$\left.\begin{array}{rcccc} x & \equiv & 1 & (\mod & 1+2i) \\ x & \equiv & 1-i & (\mod & 1+3i) \\ x & \equiv & 2i & (\mod & 3+2i) \end{array}\right\}$$

**Ejercicio 3.51.** Demostrar que la aplicación $f : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_2$ dada por $f(a + bi) = [a - b]_2$ es un homomorfismo de anillos. Calcular $Ker(f)$, dando su generador, e $Im(f)$.

**Ejercicio 3.52.** Calcular en $\mathbb{Z}[\sqrt{-2}]$ el m.c.d. y el m.c.m. de los elementos 3 y $2 + \sqrt{-2}$.

**Ejercicio 3.53.** En el anillo $\mathbb{Z}[\sqrt{-2}]$ resolver el siguiente sistema de congruencias

$$\left.\begin{array}{rcccc} x & \equiv & 1+2\sqrt{-2} & \mod & 2-3\sqrt{-2} \\ x & \equiv & 3 & \mod & 1+\sqrt{-2} \end{array}\right\}$$

**Ejercicio 3.54.** Sea $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z} \text{ y } \omega = (-1 + i\sqrt{3})/2\}$. Demuestra que es un dominio de integridad y calcula sus unidades.

**Ejercicio 3.55.** En el anillo $\mathbb{Z}[\sqrt{5}]$ comprobar que $4 = 2 \cdot 2$ y $4 = (1 + \sqrt{5})(-1 + \sqrt{5})$ son dos factorizaciones en irreducibles no equivalentes, ¿es $(1 + \sqrt{5})$ primo?.

**Ejercicio 3.56.** Sea $S = \{a + bi \,/\, a, b \in \mathbb{Z}, b \text{ es par}\}$.

- Demostrar que $S$ es un subanillo de $\mathbb{Z}[i]$.
- Demostrar que $S$ no es un ideal de $\mathbb{Z}[i]$.
- ¿Cuantos elementos tiene el anillo cociente $\mathbb{Z}[i]/(3 + i)\mathbb{Z}[i]$?. Razonar la respuesta.

**Ejercicio 3.57.** Si $D$ y $D'$ son DIP, demostrar que todo ideal de $D \times D'$ es principal aunque $D \times D'$ no es un DIP. En el caso en que $D = D' = \mathbb{Z}$ determinar el ideal generado por los elementos $(a, b)$ y $(c, d)$.

**Ejercicio 3.58.** Factorizar en irreducibles los siguientes elementos: $11 + 7i$ en $\mathbb{Z}[i]$ ; $4 + 7\sqrt{2}$ 2n $\mathbb{Z}[\sqrt{2}]$ ; $4 - \sqrt{-3}$ en $\mathbb{Z}[\sqrt{-3}]$.

**Ejercicio 3.59.** Hallar el m.c.d. y las expresiones de Bezout para las siguientes parejas de elementos de $\mathbb{Z}[i]$: $11 + 7i$ y $3 + 7i$; $8 + 6i$ y $5 - 15i$; $16 + 7i$ y $10 - 5i$.

**Ejercicio 3.60.** i) Encontrar $u$ y $v$ en $\mathbb{Z}[i]$ tales que

$$4u + (3 + 3i)v = -1 + 5i$$

.

ii) ¿Son ciertos los isomorfismos siguientes?:

$$\frac{\mathbb{Z}[i]}{(1+i)} \cong \mathbb{Z}_2 \ ; \ \frac{\mathbb{Z}[i]}{(i)} \cong \mathbb{Z} \, .$$

iii) En $\mathbb{Z}[\sqrt{-2}]$ calcular el máximo común divisor y el mínimo común múltiplo de $2 + \sqrt{-2}$ y 3.

**Ejercicio 3.61.** i) Resolver el siguiente sistema de congruencias en $\mathbb{Z}[\sqrt{-2}]$ y dar una solución de norma mayor que 7:

$$x \equiv 2 \, (\text{ mód } 1 + \sqrt{-2}) \ ; \ x \equiv \sqrt{-2} \, (\text{ mód } 3 + \sqrt{-2})$$

ii) Dar la solución general de la ecuación en $\mathbb{Z}$ $6783x + 613y = 3$.

iii) Calcular $m.c.d.(-1 + 3i, 2)$ en $\mathbb{Z}[i]$.

iv) Descomponer $-3 + 9i$ en factores primos en $\mathbb{Z}[i]$.

**Ejercicio 3.62.** i) Calcular $m.c.d.(18 - i, 11 + 7i)$ en $\mathbb{Z}[i]$.

ii) Verificar que $4 = 2{,}2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ es un ejemplo de factorización no única en elementos irreducibles en $\mathbb{Z}[\sqrt{-3}]$.

**Ejercicio 3.63.** El número de páginas de un libro es mayor que 400 y menor que 500. Si se cuentan de 2 en 2 sobra una página; si se cuentan de 3 en 3 sobran dos, si se cuentan de 5 en 5 sobran cuatro y si se cuentan de 7 en 7 sobran seis ¿Cuantas páginas tiene el libro?.

**Ejercicio 3.64.** Resolver en $\mathbb{Z}$ el siguiente sistema de congruencias:
$x \equiv 1(\text{ mód } 2); x \equiv 2(\text{ mód } 3); x \equiv 2(\text{ mód } 5); x \equiv 10(\text{ mód } 11); x \equiv 10(\text{ mód } 49)$.

**Ejercicio 3.65.** Resolver en $\mathbb{Z}[\sqrt{-2}]$ el siguiente sistema de congruencias:
$x \equiv 1 + 2\sqrt{-2}(\text{ mód } 2 - 3\sqrt{-2}); x \equiv 3(\text{ mód } 1 + \sqrt{-2})$.

**Ejercicio 3.66.** Resolver en $\mathbb{Z}$ la congruencia $3293x \equiv 222$ (mód 8991) y en $\mathbb{Z}[\sqrt{2}]$ la congruencia $(2 + \sqrt{2})x \equiv 3 - \sqrt{2}$ (mód 3).

**Ejercicio 3.67.** Despues de que una banda de 17 piratas dividiera sus doblones en partes iguales resultó que sobraban 3 doblones que decidieron dar a su cocinero chino Wun Tu; pero en una disputa murieron 6 de los piratas despues de lo cual decidieron nuevamente dividir su fortuna entre los que quedaban sobrando 4 doblones que en su momento daría a Wun Tu. Pero tuvieron un accidente y sólo quedaron 6 de los piratas, el tesoro y el cocinero chino; esta vez un reparto equitativo dió un resto de 5 doblones. Cansado de la tacañería de sus amos el buen Wun Tu aprovechó su posición de cocinero para preparar un "sabroso" estofado de setas venenosas con las que eliminó a toda la banda de forma que el tesoro pasó a ser de su propiedad. Sabiendo que el número de doblones estaba comprendido entre 1000 y 2000 y que el cocinero calzaba un número 42, calcular el número de monedas que se quedó Wun Tu.

## 3.5. Anillos y extensiones cuadráticas usando GAP

### 3.5.1. Divisores de cero

Podemos utilizar el mismo procedimiento usado anteriormente para calcular las unidades en $\mathbb{Z}_{10}$, para determinar los divisores de cero de $\mathbb{Z}_{10}$.

```
gap> Filtered([1..9],n->ForAny([1..9],m->n*m mod 10=0));
[ 2, 4, 5, 6, 8 ]
```

Por tanto, como ya sabemos $\mathbb{Z}_{10}$, no es un dominio de integridad. En GAPpodemos usar la siguiente orden para comprobarlo directamente sin calcular sus divisores de cero.

```
gap> IsIntegralRing(ZmodnZ(10));
false
```

Veamos ahora cómo podemos calcular los divisores de cero del anillo

$$\mathbb{Z}_2[i] = \{a + bi | a, b \in \mathbb{Z}_2\}.$$

Primero calculamos los elementos de $\mathbb{Z}_2[i]$. Como $i$ es la raíz cuarta de la unidad, usamos `E(4)` para representarlo.

```
gap> l:=Cartesian([0..1],[0..1]);
[ [ 0, 0 ], [ 0, 1 ], [ 1, 0 ], [ 1, 1 ] ]
gap> z2i:=Set(l,n->n[1]+n[2]*E(4));
[ 0, 1, E(4), 1+E(4) ]
```

Nos quedamos con los elementos no nulos.

```
gap> last{[2..4]};
[ 1, E(4), 1+E(4) ]
```

Seleccionamos (`Filtered`) ahora aquellos para los que exista (`ForAny`) un elemento no nulo que multiplicado por él de cero.

```
gap> Filtered(last,n->ForAny(last,m->EuclideanRemainder(n*m,2)=0));
[ 1+E(4) ]
```

Lo que indica que $1 + i$ es el único divisor de cero no nulo de $\mathbb{Z}_2[i]$. Nótese que para hacer las cuentas módulo 2, hemos usado el comando `EuclideanRemainder`, ya que con los enteros de Gauss no podemos utilizar `mod`.

### 3.5.2. Unidades

GAPtiene un comando para determinar el grupo de unidades de un anillo. Usémoslo para ver las unidades de $\mathbb{Z}_{10}$.

```
gap> Units(ZmodnZ(10));
<group with 1 generators>
```

Como la salida es un grupo, para ver sus elementos lo pasamos a lista y luego cada elemento lo representamos como un entero.

```
gap> List(last,Int);
[ 1, 3, 7, 9 ]
```

También podemos optar por la fuerza bruta, y ver para qué enteros entre 1 y 9, existe otro de forma que su producto de 1 módulo 10.

```
gap> Filtered([1..9],n->ForAny([1..9],m->n*m mod 10=1));
[ 1, 3, 7, 9 ]
```

Además GAPtiene un comando para determinar si un anillo es o no un cuerpo.

```
gap> IsField(ZmodnZ(5));
true
```

### 3.5.3. Enteros de Gauss

Ya hemos visto en prácticas anteriores cómo factorizar enteros de Gauss. También vimos cómo calcular el cociente y resto de dos enteros cualesquiera, así como su máximo común divisor y los coeficientes de Bézout correspondientes. Por desgracia, como hemos visto anteriormente, la función `mod` no se puede utilizar con los enteros de Gauss. Podemos usar en su lugar, `EuclideanRemainder` y `EuclideanQuotient` para el cociente, o bien, `QuotientRemainder` si queremos obtener ambas cantidades a la vez.

```
gap> (9+7*E(4)) mod (1+E(4));
Error, no method found! For debugging hints type ?Recovery from NoMethodFound
Error, no 1st choice method found for `MOD' on 2 arguments called from
<function>( <arguments> ) called from read-eval-loop
Entering break read-eval-print loop ...
you can 'quit;' to quit to outer loop, or
you can 'return;' to continue

gap> (9+7*E(4))/(1+E(4));
8-E(4)

gap> QuotientRemainder(9+7*E(4),1+E(4));
[ 8-E(4), 0 ]

gap> QuotientRemainder(9+7*E(4),3+E(4));
[ 3+E(4), 1+E(4) ]
gap> (9+7*E(4))/(3+E(4));
17/5+6/5*E(4)
```

Para el máximo común divisor y coeficientes de Bézout, podemos usar las funciones que conocemos para enteros.

```
gap> Gcd(2*E(4),3-7*E(4));
1+E(4)
gap> GcdRepresentation(2*E(4),3-7*E(4));
[ 2-4*E(4), -E(4) ]
```

Para encontrar los enteros de Gauss de norma menor o igual que cinco que sean irreducibles, podemos usar la función `Norm`.

Primero generamos los posibles candidatos, que tienen que tener parte real e imaginaria menor o igual que 2 en valor absoluto.

```
gap> elementos:=List(Cartesian([-2..2],[-2..2]),n->n[1]+E(4)*n[2]);
[ -2-2*E(4), -2-E(4), -2, -2+E(4), -2+2*E(4), -1-2*E(4), -1-E(4), -1,
  -1+E(4), -1+2*E(4), -2*E(4), -E(4), 0, E(4), 2*E(4), 1-2*E(4), 1-E(4), 1,
  1+E(4), 1+2*E(4), 2-2*E(4), 2-E(4), 2, 2+E(4), 2+2*E(4) ]
```

Seleccionamos ahora aquellos con norma menor o igual que cinco.

```
gap> Filtered(elementos,n->(Norm(n)<=5));
[ -2-E(4), -2, -2+E(4), -1-2*E(4), -1-E(4), -1, -1+E(4), -1+2*E(4), -2*E(4),
  -E(4), 0, E(4), 2*E(4), 1-2*E(4), 1-E(4), 1, 1+E(4), 1+2*E(4), 2-E(4), 2,
  2+E(4) ]
```

Si escribimos,

```
gap> Filtered(last,IsPrime);
[ -2-E(4), -2, -2+E(4), -1-2*E(4), -1-E(4), -1+E(4), -1+2*E(4), 1-2*E(4),
  1-E(4), 1+E(4), 1+2*E(4), 2-E(4), 2, 2+E(4) ]
```

la salida no es la correcta, ya que por ejemplo nos aparecen 2 y $-2$, que sabemos que no son irreducibles en $\mathbb{Z}[i]$. Esto se debe a que no hemos especificado el anillo en la orden `IsPrime`.

```
gap> Filtered(last,n->IsPrime(GaussianIntegers,n));
[ -2-E(4), -2+E(4), -1-2*E(4), -1-E(4), -1+E(4), -1+2*E(4), 1-2*E(4), 1-E(4),
  1+E(4), 1+2*E(4), 2-E(4), 2+E(4) ]
```

Si queremos saber cuántos tenemos salvo asociados, usamos la función `StandardAssociate` (que da un asociado estándar a cada elemento de $\mathbb{Z}[i]$) junto con la operación `Set` para eliminar repetidos.

```
gap> Set(last,StandardAssociate);
[ 1+E(4), 1+2*E(4), 2+E(4) ]
```

Obsérvese que la salida es la misma si hacemos lo siguiente (+por qué?).

```
gap> elementos:=List(Cartesian([0..2],[0..2]),n->n[1]+E(4)*n[2]);
[ 0, E(4), 2*E(4), 1, 1+E(4), 1+2*E(4), 2, 2+E(4), 2+2*E(4) ]
gap> Filtered(elementos,n->(Norm(n)<=5));
[ 0, E(4), 2*E(4), 1, 1+E(4), 1+2*E(4), 2, 2+E(4) ]
gap> Filtered(last,n->IsPrime(GaussianIntegers,n));
[ 1+E(4), 1+2*E(4), 2+E(4) ]
```

### 3.5.4. Operaciones en $\mathbb{Z}[\sqrt{(d)}]$, $d \in \{-1, 2, -2, 3\}$

Si introducimos la expresión

```
gap> (1+2*Sqrt(3))*(Sqrt(3));
-6*E(12)^4-E(12)^7-6*E(12)^8+E(12)^11
```

obtenemos una salida un poco difícil de tratar. Es por eso que vamos a definir nuestros propios productos, cociente y resto. Vamos representar un entero $a + b\sqrt{d}$ en $\mathbb{Z}[d]$ (con $d$ libre de cuadrados) mediante una lista $[a, b]$, y pasaremos $d$ como argumento extra en nuestras funciones. Así la función producto podría definirse como sigue.

```
por:=function(x,y,d)
    return [x[1]*y[1]+d*x[2]*y[2],x[1]*y[2]+x[2]*y[1]];
end;

gap> por([1,2],[0,1],3);
[ 6, 1 ]

gap> (1+2*Sqrt(3))*(Sqrt(3));
-6*E(12)^4-E(12)^7-6*E(12)^8+E(12)^11
gap> 6+Sqrt(3);
-6*E(12)^4-E(12)^7-6*E(12)^8+E(12)^11
```

Para hacer el cociente, necesitamos la norma. Vamos a definir una función para tal efecto, aunque como explicamos después, también se puede hacer definiendo el cuerpo $\mathbb{Q}(\sqrt{(d)})$.

```
norma:=function(x,d)
    return AbsInt(x[1]^2-d*x[2]^2);
end;

gap> norma([4,1],3);
13
gap> F:=Field(Sqrt(3));
NF(12,[ 1, 11 ])
gap> Norm(F,4+Sqrt(3));
13
```

Hay que tener cuidado con especificar en qué cuerpo estamos si usamos `Norm` para no obtener resultados no deseados.

```
gap> Norm(4+Sqrt(3));
169
```

Como hemos visto en teoría, para dividir, necesitamos aproximarnos a un racional lo mejor que podamos con un entero. Para ello introducimos una función de redondeo.

```
redondeo:=function(x)
    if ((x-Int(x))<(Int(x)+1-x)) then
        return Int(x);
    fi;
    return Int(x)+1;
end;

gap> redondeo(2/3);
1
gap> redondeo(1/3);
0
```

Usando la función auxiliar

```
conjugado:=function(x)
    return [x[1],-x[2]];
end;
```

podemos definir la función cociente de la siguiente forma.

```
cociente:=function ( x, y, d )
    return List( por( x, conjugado( y ), d ) / norma( y, d ), redondeo );
end;

gap> cociente([11,7],[1,1],-1);
[ 9, -2 ]
gap> (11+7*E(4))/(1+E(4));
9-2*E(4)
```

Por tanto, una función resto ya es bastante fácil de obtener.

```
resto:=function(x,y,d)
    return x-por(y,cociente(x,y,d),d);
end;

gap> resto([11,7],[1,1],-1);
[ 0, 0 ]
gap> EuclideanRemainder(11+7*E(4),1+E(4));
0
```

## 3.6. Aritmética en extensiones cuadráticas de $\mathbb{Z}$ con MATHEMATICA

### 3.6.1. Generalidades

Las siguientes funciones calculan unidades y divisores de $\mathbb{Z}_n$. Utilizamos la función **Range** y otras funciones conocidas.

Notemos que, por ejemplo,

```
In[1] := Range[1, 10]
Out[1] = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}
```

Entonces

```
In[2]:= unidadesZ[n_]:=Select[Range[1,n-1],GCD[#,n]==1&]
In[3]:= divisoresdeceroZ[n_]:=Select[Range[1,n-1], MemberQ[Mod[#Range[1,n-1],n], 0]&]
```

Así

```
In[4] := divisoresdeceroZ[10]
Out[4] = {2, 4, 5, 6, 8}
```

mientras que

```
In[5]:= unidadesZ[4]
Out[5]= {1,3}


\subsection{El anillo de los enteros de Gauss $\Z[i]$}

Comenzaremos con el anillo de enteros de Gauss y en la siguiente sección analizaremos otros dominios cu

Destacamos en principio que Mathematica trabaja con enteros de Gauss usando las mismas  funciones que c

Así, directamente, podemos calcular con enteros de Gauss, resto, cociente y máximo común divisor y coef

Ejemplos

\begin{verbatim}
In[6]:= Mod[9+7I,1+I]
Out[6]= 0

In[7]:= Mod[1+2I,1+I]
Out[7]= -1

In[8]:= Quotient[9+7I,1+I]
Out[8]= 8-I

In[9]:= Quotient[1+2I,1+I]
Out[9]= 2

In[10]:= ExtendedGCD[1+2I,1+I]
```

```
Out[10]= {1,{-1,2}}

In[11]:= ExtendedGCD[2I,3-7I]
Out[11]= {1+I,{2-4 I,-I}}

In[12]:= FactorInteger[8+10I,GaussianIntegers->True]
Out[12]= {{-I,1},{1+I,2},{4+5 I,1}}
```

**Algunas funciones básicas**

Las funciones `Re` e `Im` aplicadas a un número complejo devuelven respectivamente la parte real y la imaginaria de dicho número.

Ejemplos:

```
In[13]:= Re[2+3I]
Out[13]= 2

In[14]:= Im[2+3I]
Out[14]= 3
```

La función `Round` aplicada a un número complejo devuelve el entero de Gauss más cercano a él.

Ejemplo:

```
In[15]:= Round[3/5+9/7I]
Out[15]= 1+I
```

Usando la función `FactorInteger` podemos definir una función que factoriza un entero de gauss en primos:

```
In[16]:= factoriza[x_]:=FactorInteger[x, GaussianIntegers-> True]
```

Ejemplo

```
In[17]:= factoriza[1+3I]
Out[17]= {{1+I,1},{2+I,1}}
```

La función `Norm` devuelve la raíz cuadrada de la norma del entero de Gauss.

Ejemplo

```
In[18]:= Norm[1+2I]
Out[18]= Sqrt[5]
```

**Usando la función `Norm` seleccionar enteros de Gauss de norma menor que** 5

.

Para ello, empezamos buscando candidatos con norma menor que 5 poniendo

```
In[19]:= n5=Table[a+b I,{a,0,2},{b,0,2}]
Out[19]= {{0,I,2 I},{1,1+I,1+2 I},{2,2+I,2+2 I}}
{{0,I,2 I},{1,1+I,1+2 I},{2,2+I,2+2 I}}
```

Convertimos la tabla en una lista

```
In[20]:= n5lista=Flatten[n5]
Out[20]= {0,I,2 I,1,1+I,1+2 I,2,2+I,2+2 I}
{0,I,2 I,1,1+I,1+2 I,2,2+I,2+2 I}
```

Y en esta lista seleccionamos los elementos que tienen norma menor que 5 (según nuestra definición de norma)

```
In[21]:= n5listamenor=Select[n5lista,Norm[#]^2<=5&]
Out[21]= {0,I,2 I,1,1+I,1+2 I,2,2+I}
{0,I,2 I,1,1+I,1+2 I,2,2+I}
```

Usando la función `PrimeQ` podemos definir una función que nos dice si un entero de Gauss es primo,

```
In[22]:= primo[x_]:=PrimeQ[x,GaussianIntegers-> True]
```

Ejemplo

```
In[23]:= primo[2+I]
Out[23]= True
```

Ahora podemos seleccionar en nuestra lista los elementos que son primos poniendo

```
In[24]:= Select[n5listamenor,primo]
Out[24]= {1+I,1+2 I,2+I}
{1+I,1+2 I,2+I}
```

**Las funciones cociente, módulo y gextendidomcd**

Definimos a continuación funciones alternativas a las predefinidas para calcular cociente, resto, máximo comun divisor y coeficientes de Bezout.

Par definir una función `cociente[x,y]` que devuelva el cociente en $\mathbb{Z}[i]$ de los elementos $x$ e $y$.

```
In[25]:= cociente[x_,y_]:=Round[x/y]
```

Ejemplo

```
In[26]:= cociente[3+2I,2+I]
Out[26]= 2

In[27]:= Quotient[3+2I,2+I]
Out[27]= 2
```

Para definir una función modulo[x,y] que devuelva el resto de la división de x por y.

```
In[28]:= modulo[x_,y_]:=x-y*cociente[x,y]
```

Ejemplo

```
In[29]:= modulo[5+7I,2+3I]
Out[29]= 1+I

In[30]:= Mod[5+7I,2+3I]
Out[30]= 1+I
```

Para definir una función auxiliar gextendidomcd[x,y,u0,u1,v0,v1] que calcule el máximo común divisor de x e y y los coeficientes de Bezout:

```
In[31]:= gextendidomcd[x_,0,u0_,u1_,v0_,v1_]:={x,{u0,v0}}
gextendidomcd[x_,y_,u0_,u1_,v0_,v1_]:=gextendidomcd[y, \
modulo[x,y],u1,u0-u1*cociente[x,y],v1,v0-v1*cociente[x,y]]
```

Ejemplo

```
In[33]:= gextendidomcd[5+7I,3+2I,1,0,0,1]
Out[33]= {1,{1,-2-I}}

In[34]:= ExtendedGCD[5+7I,3+2I,1,0,0,1]
Out[34]= {1,{1,-2-I}}
```

### 3.6.2. Congruencias y Sistemas de congruencias

Queremos definir una función que calcule las soluciones de la ecuación $ax \equiv b \pmod{n}$ ( donde $a, b, n \in \mathbb{Z}[i]$)

Recordamos que la congruencia anterior tiene solución si y solo si $d = \text{m. c. d.}(a, n)$ divide a $b$. En este caso, si escribimos $d = ua + vn$ con $b = db'$, sabemos que una solución de la congruencia es $x = ub'$. Entonces ponemos

```
In[35]:= Solucion[a_,b_,n_]:= With[{d=GCD[a,n]}, ExtendedGCD[a,n][[2,1]]*b/d /; Mod[b,GCD[a,n]] =
         Solucion[_,_,_]:= Print["La congruencia no tiene solucion"]]
```

o alternativamente usando la función auxiliar antes definida

```
In[37]:= solucion[a_,b_,n_]:=If[modulo[b,gextendidomcd[a,n,1,0,0,1][[1]]]==0,\
gextendidomcd[a,n,1,0,0,1][[2,1]]*cociente[b,gextendidomcd[a,n,1,0,0,\
1][[1]]], Print["La congruencia no tiene solucion"]]
```

Así, si buscamos la solución de la congruencia $(6 + 2I)x \equiv 1 + I \pmod{4 + 10I}$

```
In[38]:=Solucion[6+2I,1+I,4+10I]
 La congruencia no tiene solucion
```

o bien

```
In[39]:=solucion[6+2I,1+I,4+10I]
 La congruencia no tiene solucion
```

Notemos que

```
In[40] := GCD[6+2 I, 4+10 I]
Out[40] = 2
```

y que

```
In[41] := Mod[1 + I, 2]
Out[41] = 1 + i
```

por lo que $1 + I$ no es divisible por 2
Por otro lado

```
In[42] := Solucion[6 + 2 I, 2 - 2 I, 4 + 10 I]
Out[42] = 2 i
```

o bien

```
In[43] := solucion[6 + 2 I, 2 - 2 I, 4 + 10 I]
Out[43] = 2 i
```

Comprobamos el resultado haciendo

```
In[44] := Mod[(6 + 2 I) 2 I - (2 - 2 I), 4 + 10 I]
Out[44] = 0
```

Para definir una función que calcule las soluciones de un sistema de dos congruencias

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \end{aligned}$$

recordamos que dicho sistema tiene solución si y solo si $b_1 \equiv b_2 \pmod{\text{m. c. d.}(n_1, n_2)}$, en cuyo caso, para obtener una solución resolvemos primero la ecuación $n_1 t \equiv b_2 - b_1 \pmod{n_2}$. Si $t_0$ es una solución de esta ecuación, entonces una solución del sistema estará dada por $x_0 = b_1 + t_0 n_1$. Tomamos:

```
In[45]:= Sistema[{b1_,b2_},{n1_,n2_}]:= b1 + n1*solucion[n1,b2-b1,n2] /; Mod[b1-b2, GCD[n1,n2]] == 0
         Sistema[_,_] := Print["El sistema no tiene solucion"]]
```

o alternativamente

```
In[47]:= sistema[{b1_,b2_},{n1_,n2_}]:= \
If[modulo[b1-b2,gextendidomcd[n1,n2,1,0,0,1][[1]]]==0,b1+n1*solucion[\
n1,b2-b1,n2],Print["El sistema no tiene solucion"]]
```

Así, si buscamos la solución del sistema

$$\begin{aligned} x &\equiv 3 + 2I \pmod{2 + 4I} \\ x &\equiv 1 + I \pmod{2 + I} \end{aligned}$$

```
In[48]:= Sistema[{3+2I,1+I},{2+4I,2+I}]
Out[48]= 3+12 I
```

o bien

```
In[49]:= sistema[{3+2I,1+I},{2+4I,2+I}]
Out[49]= 3+12 I
```

Comprobamos

```
In[50] := Mod[3 + 12 I - (3 + 2 I, I + I), {2 + 4 I, 2 + I }]
Out[50] = {0, 0}
```

Por otro lado para el sistema

$$\begin{aligned} x &\equiv 1+I \pmod{2+2I} \\ x &\equiv 1+2I \pmod{4+8I} \end{aligned}$$

tenemos

```
In[51]:= Sistema[{1+I,1+2I},{2+2I,4+8I}]
 El sistema no tiene solucion
```

o bien

```
In[52]:= sistema[{1+I,1+2I},{2+2I,4+8I}]
 El sistema no tiene solucion
```

Esta función nos permite definir a continuación, por recurrencia, una función que devuelve la solución de un sistema general de congruencias.

Para definir una función que recursivamente calcule las soluciones de un sistema de r congruencias en $\mathbb{Z}[i]$

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\cdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

```
In[53]:= SCongruencias[{a1_,a2_},{n1_,n2_}]:=Sistema[{a1,a2},{n1,n2}]
SCongruencias[{a1_,a2_,a3__},{n1_,n2_,n3__}]:=SCongruencias[{Sistema[{\
a1,a2},{n1,n2}],a3},{n1*n2/GCD[n1,n2],n3}]
```

o bien

```
In[55]:= sCongruencias[{a1_,a2_},{n1_,n2_}]:=sistema[{a1,a2},{n1,n2}]
sCongruencias[{a1_,a2_,a3__},{n1_,n2_,n3__}]:=sCongruencias[{sistema[{\
a1,a2},{n1,n2}],a3},{n1*n2/gextendidomcd[n1,n2,1,0,0,1][[1]],n3}]
```

Así, si buscamos la solución del sistema

$$\begin{aligned} x &\equiv 213+I \pmod{3+2I} \\ x &\equiv 1+15I \pmod{1+2I} \\ x &\equiv 7+5I \pmod{2+I} \end{aligned}$$

```
In[57] := SCongruencias[{213+I,1+15I,7+5I}, {3+2I,1+2I,2+I}]
Out[57] = 1899-4439 I
```

o bien

```
In[58] := sCongruencias[{213+I,1+15I,7+5I}, {3+2I,1+2I,2+I}]
Out[58] = 1899-4439 I
```

Comprobamos

```
In[59] := Mod[% - {213 + I, 1 + 15 I, 7 + 5 I}, {3 + 2 I, 1 + 2 I, 2 + I}]
Out[59] = {0, 0, 0}
```

### 3.6.3. Los dominios cuadráticos $\mathbb{Z}[\sqrt{d}]$, $d \in \{-1, -2, 2, 3\}$

Notemos que, para los valores apuntados $d \in \{-1, -2, 2, 3\}$, los dominios $\mathbb{Z}[\sqrt{d}]$ son dominios euclideos con función euclidea definida por la norma que mas abajo recordamos.

El elemento $a+b\sqrt{d}$ lo vamos a representar por $\{a, b\}$. Empezamos definiendo las funciones elementales de producto y norma:

```
In[60]:= por[{x_,y_},{z_,t_},d_]:={x z+ d y t,x t +y z}
```

Ejemplo: El producto $(1 + 2\sqrt{-2})(2 + \sqrt{-2})$ lo obtenemos poniendo

```
In[61]:= por[{1,2},{2,1},-2]
Out[61]= {-2,5}
```

Así que la solución es $-2 + 5\sqrt{-2}$
En cuanto a la norma, definimos

```
In[62]:= norma[{x_,y_},d_]:=x^2-d y^2
```

Ejemplo

```
In[63]:= norma[{2,1},-2]
Out[63]= 6

In[64]:= norma[{2,-1},3]
Out[64]= 1
```

Para definir el cociente, usamos la función de redondeo una vez que hemos multiplicado por el conjugado así que ponemos

```
In[65]:= cociente[{x_,y_},{z_,t_},d_]:=Round[por[{x,y},{z,-t},d]/norma[{z,t},d]\
];
```

Ejemplo: El cociente $(-2 + 5\sqrt{[-2)}/(1 + 3\sqrt{-2})$ lo obtenemos poniendo

```
In[66]:= cociente[{-2,5},{1,3},-2]
Out[66]= {1,1}
```

Una vez que tenemos el cociente, el resto lo obtenemos con la función.

```
In[67]:= resto[{x_,y_},{z_,t_},d_]:={x,y}-por[{z,t},cociente[{x,y},{z,t},d],d]
```

Así, el resto de dividir $2 + 5\sqrt{3}$ entre $4 - 3\sqrt{3}$ lo obtenemos poniendo

```
In[68]:= resto[{2,5},{4,-3},3]
Out[68]= {4,-2}
```

mientras que

```
In[69]:= resto[{11,7},{3,7},-1]
Out[69]= {1,3}
```

Se propone como ejercicio final encontrar solución a los ejercicios propuestos en la sección 3.4 que puedan ser resueltos utilizando las funciones definidas en esta práctica.

# Capítulo 4

# Polinomios

## 4.1. Definiciones y primeras propiedades

Sea $A$ un anillo conmutativo.

**Definición 4.1.1.** El *conjunto de polinomios* en la indeterminada $X$ con coeficientes en $A$ es el conjunto de todas las sumas formales finitas

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

Este conjunto se representa por $A[X]$.

Obsérvese que $X$ *no es una variable*. Es un elemento nuevo, indeterminado que no representa a ningún elemento de $A$ (Al final de la edad media y en el renacimiento le llamaban "la cosa", y los que manipulaban la cosa ,i.e. los algebristas, se llamaban "cosistas").

En el conjunto de polinomios definimos una suma y un producto: Sean

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$
$$g = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0$$

dos polinomios. Supongamos que $m \leq n$, Tomamos $b_i = 0$ para todo $n \geq i > m$. Con este convenio definimos

$$f + g = (a_n + b_n)X^n + \cdots + (a_1 + b_1)X + (a_0 + b_0).$$
$$fg = a_n b_m X^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) X^{n+m-1} +$$
$$\cdots + (a_1 b_0 + a_0 b_1)X + a_0 b_0$$

**Teorema 4.1.2.** *El conjunto $A[X]$ con las dos operaciones definidas forma un anillo conmutativo que se llama* anillo de polinomios en $X$ con coeficientes en $A$.

**Lema 4.1.3.** *La aplicación $\lambda : A \to A[X]$ definida por $\lambda(a) = a$ es un monomorfismo de anillos.*

Normalmente se identifica cada elemento $a \in A$ con el polinomio $\lambda(a) \in A[X]$, con lo que $A$ es un subanillo de $A[X]$.

**Definición 4.1.4.** Para un polinomio $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \neq 0$ el mayor índice $n$ tal que $a_n \neq 0$ se llama *grado de* $f$ y se representa por $gr(f)$. Si $f = 0$ definimos $gr(f) = -\infty$.

Cada uno de los sumandos $a_iX^i$ se llama *monomio o término (de grado i)* del polinomio $f$.

El término no nulo de mayor grado se llama *término líder*. El coeficiente $a_n \neq 0$ del término líder se llama *coeficiente líder* y el término de grado cero $a_0$ se llama *término constante*.

Un polinomio $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ cuyo coeficiente líder vale 1 se llama *polinomio mónico*.

Un polinomio $f$ se llama *constante* si $gr(f) \leq 0$, es decir, cuando $f \in \mathrm{Im}(\lambda)$.

**Teorema 4.1.5.** *Para cualquier anillo conmutativo $A$ y cualesquiera polinomios $f, g \in A[X]$ se verifica*

$$gr(f+g) \leq \text{máx}(gr(f), gr(g))$$
$$gr(fg) \leq gr(f) + gr(g)$$

*Si $gr(f) \neq gr(g)$ se verifica*

$$gr(f+g) = \text{máx}(gr(f), gr(g))$$

*Si $A$ es un dominio de integridad se verifica*

$$gr(fg) = gr(f) + gr(g)$$

**Corolario 4.1.6.** *El anillo conmutativo $A$ es un dominio de integridad si y sólo si $A[X]$ es un dominio de integridad.*

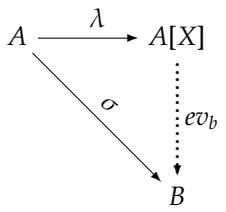
En cualquier dominio de integridad es importante determinar el grupo de unidades y los elementos irreducible y primos, para poder estudiar sus propiedades de divisibilidad. En este sentido los primeros resultados son los siguientes:

**Proposición 4.1.7.**
1. *Sea $A$ un dominio de integridad. Los elementos invertibles de $A[X]$ son exactamente los invertibles de $A$*
2. *Todo polinomio $X - a \in A[X]$ es irreducible.*

La propiedad mas importante de un anillo de polinomios es la siguiente:

**Teorema 4.1.8** (Propiedad universal del anillo de polinomios)**.** *Sea $A$ un anillo conmutativo, $\lambda : A \to A[X]$ la inclusión de $A$ en el anillo de polinomios. Para todo anillo conmutativo $B$, todo homomorfismo de anillos $\sigma : A \to B$ y todo elemento $b \in B$ existe un único homomorfismo de anillos $ev_b : A[X] \to B$ tal que $(ev_b)\lambda = \sigma$ y $ev_b(X) = b$.*

Esta propiedad se visualiza mejor en un diagrama: Dadas $\lambda$ y $\sigma$ existe un único $ev_b$ que hace el siguiente diagrama conmutativo y aplica $X$ en $b$:




*Demostración.* Sea $f = \sum_{i=0}^{n} a_iX^i$. Definimos $ev_b(f) = \sum_{i=0}^{n} \sigma(a_i)b^i$, es decir, aplicamos $\sigma$ a todos los coeficientes de $f$, sustituimos $X$ por $b$ y realizamos en $B$ las operaciones indicadas. Es rutina comprobar que $ev_b$ es un homomorfismo de anillos, que

$$ev_b(X) = b$$

y que $ev_b \cdot \lambda = \sigma$.

Sea ahora $\tau : A[X] \to B$ otro homomorfismo de anillos que verifique las mismas propiedades y sea $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ arbitrario. Entonces

$$\tau(f) = \tau(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \tau(a_i)\tau(X)^i = \sum_{i=0}^{n} \sigma(a_i)b^i = ev_b(f)$$

luego $\tau = ev_b$ es único. □

El morfismo $ev_b$ del teorema anterior se llama *morfismo de evaluación en b*. Se aplica sobre todo cuando $\sigma$ es una inclusión, es decir que para todo $a \in A$, $\sigma(a) = a$. En este caso $ev_b(a_n X^n + \cdots + a_1 X + a_0) = a_n b^n + \cdots + a_1 b + a_0$ es el resultado de *evaluar f en b* y se representa por $ev_b(f) = f(b)$.

**Definición 4.1.9.** Un elemento $a \in A$ se llama *cero* o *raíz* de $f$ si $f(a) = 0$.

Todo polinomio $f \in A[X]$ define una *aplicación polinómica* $\bar{f} : A \to A$ mediante $\bar{f}(a) = f(a)$. En general, distintos polinomios pueden definir la misma aplicación polinómica.

*Ejemplo* 4.1.10. Sea $A = \mathbb{Z}_2$ el anillo de las clases de restos módulo 2. Sean $f = 0$, $g = X^2 + X$, $h = X^3 + X$ polinomios de $\mathbb{Z}_2[X]$. Como polinomios son *distintos*, pero los tres definen la misma función polinómica $\mathbb{Z}_2 \to \mathbb{Z}_2$, a saber la función que aplica todo elemento (sólo hay dos) de $\mathbb{Z}_2$ en el cero de $\mathbb{Z}_2$.

El proceso de construir el anillo de polinomios en una indeterminada puede aplicarse a cualquier anillo conmutativo, en particular a un mismo anillo de polinomios $A[X]$: Sea $Y$ otra indeterminada. Definimos $A[X, Y] = A[X][Y]$, el anillo de polinomios en dos indeterminadas con coeficientes en $A$. Sus elementos son de la forma

$$f = \sum_{i,j} a_{ij} X^i Y^j$$

donde la suma es finita (En lugar de ello se suele decir que tomamos la suma sobre todos los pares $i, j$ pero con $a_{ij} = 0$ *para casi todo par* $(i, j)$, es decir, para todos excepto un conjunto finito).

Mas generalmente, definimos inductivamente el anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ por la regla

$$A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$$

. En otras palabras, consideramos a los elementos de $A[X_1, \ldots, X_n]$ como polinomios en $X_n$ con coeficientes en $A[X_1, \ldots, X_{n-1}]$. Naturalmente existe un monomorfismo $\lambda : A \to A[X_1, \ldots, X_n]$ y $A$ se identifica con el subanillo $\mathrm{Im}(\lambda)$ de $A[X_1, \ldots, X_n]$.

**Lema 4.1.11.** *El anillo conmutativo A es un dominio de integridad si y sólo si lo es* $A[X_1, \ldots, X_n]$

*Demostración.* Inducción sobre $n$. □

De la definición tenemos que todo elemento $f$ de $A[X_1, \ldots, X_n]$ se escribe de manera única como

$$f = \sum a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$$

Aquí $a_{i_1 \ldots i_n}$ esta determinado de manera única como el coeficiente en $f$ del monomio $X_1^{i_1} \ldots X_n^{i_n}$. Formalmente la suma anterior es infinita, pero de hecho sólo un número finito de coeficientes son distintos de cero. Ya que las indeterminadas conmutan entre sí con los elementos de $A$, el anillo $A[X_1, \ldots, X_n]$ depende simétricamente de las $X_i$; así que $X_n$ no juega ningún papel especial. Podíamos haber escrito $f$ como un polinomio en $X_1$ con coeficientes en $A[X_2, \ldots, X_n]$ o escoger cualquier otra $X_i$.

**Definición 4.1.12.** Cada producto $M_i = X_1^{i_1} \ldots X_n^{i_n}$ se llama *monomio primitivo*; el término correspondiente $a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$ se llama *monomio* o *término monomial*; su *grado total* (o sencillamente *grado*) es $\sum i_j$, y el *grado en* $X_j$ es $i_j$. El *grado de* $f$ es el máximo de los grados de sus términos no nulos.

Por ejemplo $f = 2X_1^5X_2^3X_3 - X_1^2X_3^3 + 7X_2^6$ es de grado 5 en $X_1$, de grado 6 en $X_2$ y de grado 3 en $X_3$; el grado total de $f$ es 9.

**Definición 4.1.13.** Un polinomio en el que todos los términos tienen el mismo grado total se llama *polinomio homogéneo* o también una *forma*. En una indeterminada las únicas formas son los monomios, pero ya para dos indeterminadas puede haber otros, por ejemplo las forma cuadráticas $aX^2 + bXY + cY^2$.

Un criterio práctico de homogeneidades es el siguiente

**Lema 4.1.14.** *El polinomio $f \in A[X_1, \dots, X_n]$ es homogéneo de grado $k$ si y sólo si para otra indeterminada $t$ se verifica que*

$$f(tX_1, \dots, tX_n) = t^k f(X_1, \dots, X_n).$$

A veces es conveniente ordenar los monomios. Incluso para propósito tan sencillo como escribir la expresión total de un polinomio es necesario un orden total de los monomios. Con frecuencia se usa el *orden lexicográfico* definido así: Entre monomios de distinto grado grado total, el de mayor grado precede al de menor grado. Entre monomios del mismo grado total, el monomio $X_1^{i_1} \dots X_n^{i_n}$ precede a $X_1^{j_1} \dots X_n^{j_n}$ si la primera diferencia no nula $i_1 - j_1, \dots i_n - j_n$ es positiva.

Por ejemplo, $X_1^3X_2X_3^2$ precede a $X_1^3X_3^3$ y es precedido por $X_1^3X_2^2X_3$. En cualquier polinomio, el primer término monomial (en el orden lexicográfico) entre los términos de grado máximo se llama el *término líder*

## 4.2. El algoritmo de la división con resto

**Teorema 4.2.1** (Algoritmo general de división)**.** *Sea $A$ un anillo conmutativo y sean $f, g \in A[X]$ con el coeficiente líder de $g$ invertible. Entonces existen únicos $q, r \in A[X]$ tales que $f = qg + r$ y $gr(r) < gr(g)$.*

*Demostración.* Inducción sobre $gr(f)$. Sean $f = a_nX^n + \cdots + a_1X + a_0$ y $g = b_mX^m + \cdots + b_0$. Si $gr(f) < gr(g)$, tomamos $q = 0$ y $r = f$. Sea ahora $gr(f) = n \geq gr(g) = m$. Definimos

$$f_1 = f - (a_nb_m^{-1})X^{n-m}g \tag{4.2.1}$$

Es inmediato que $gr(f_1) < gr(f)$ y por inducción existen $q_1, r \in A[X]$ tales que $f_1 = q_1g + r$ con $gr(r) < gr(g)$. Despejando en 4.2.1 vemos que

$$f = (a_nb_m^{-1})X^{n-m}g + f = ((a_nb_m^{-1})X^{n-m}g + q_1)g + r$$

Definimos $q = (a_nb_m^{-1})X^{n-m}g + q_1$ y tenemos demostrada la existencia de cociente y resto.

Para ver la unicidad, sea $f = qg + r = q_1g + r_1$. Trasponiendo términos tenemos $(q - q_1)g = r_1 - r$. Como el coeficiente líder de $g$ es invertible se verifica

$$gr(g) > \text{máx}(gr(r), gr(r_1) \geq gr(r - r_1) = gr((q - q_1)g) = gr(q - q_1) + gr(g)$$

lo que implica que $gr(q - q_1) = -\infty$ y $q - q_1 = 0$. Luego $q = q_1$ y por tanto $r = r_1$. □

**Corolario 4.2.2.** *Sea $K$ un cuerpo. Entonces $K[X]$ es un anillo euclídeo*

*Demostración.* En un cuerpo, todo elemento no nulo es invertible. Así que para todo polinomio no nulo $g$ el coeficiente líder es invertible. Por el teorema anterior, para cualesquiera polinomios $f, g$ con $g \neq 0$ existen únicos $q, r$ tales que $f = qg + r$ con $gr(r) < gr(g)$. Esta es la segunda condición en la definición de anillo euclídeo.

Por otro lado todo cuerpo es un dominio de integridad, así que para dos polinomios no nulos $f, g$ se verifica $gr(fg) = gr(f) + gr(g) \geq gr(f)$. esta es la primera condición de dicha definición

Por tanto $K[X]$ es euclídeo respecto a la función grado. □

**Corolario 4.2.3** (Teorema del resto)**.** *Sea $A$ un anillo conmutativo, $a$ un elemento de $A$ y $f \in A[X]$ un polinomio. Entonces existe un $q \in A[X]$ tal que*

$$f = (X - a)q + f(a)$$

*y $(X - a)$ divide a $f$ si y sólo si $f(a) = 0$.*

**Teorema 4.2.4.** *Sea $A$ un dominio de integridad y sea $f \in A[X]$. Sean $a_1, \ldots, a_m \in A$ elementos distintos tales que $f(a_i) = 0$ para $i = 1, \ldots m$. Entonces $((X - a_1) \ldots (X - a_m))$ divide a $f$.*

*Demostración.* Inducción sobre $m$. Para $m = 1$ esto es parte del teorema del resto. Sea $m > 1$. Por inducción $f = (X - a_1) \ldots (X - a_{m-1})g$ con $g \in A[X]$. Evaluamos en $a_m$:

$$0 = f(a_m) = (a_m - a_1) \ldots (a_m - a_{m-1})g(a_m)$$

Como los $a_i$ distintos, $a_m - a_i \neq 0$ para $i = 1, \ldots m - 1$. Como $A$ es un dominio de integridad, $g(a_m) = 0$. Por el teorema del resto $g = (X - a_m)g_1$. Sustituyendo en la expresión de $f$ nos queda $f = (X - a_1) \ldots (X - a_{m-1})(X - a_m)g_1$ y por tanto el producto $((X - a_1) \ldots (X - a_m))$ divide a $f$. □

**Corolario 4.2.5.** *Sea $A$ un dominio de integridad y $f \in A[X]$, $f \neq 0$. El número de raíces de $f$ en $A$ es menor o igual al grado de $f$.*

*Ejemplo* 4.2.6. El teorema y corolarios anteriores son falsos para anillos conmutativos generales: Sea $f = X^2 - 1 \in \mathbb{Z}_8[X]$. En $\mathbb{Z}_8$ el polinomio $f$ tiene cuatro raíces distintas: $1, 3, 5, 7$. Además $(X - 1)(X - 3)$ no divide a $f$.

**Corolario 4.2.7.** *Sea $A$ un dominio de integridad, $a_1, \ldots, a_{n+1}$ elementos distintos de $A$ y $f, g \in A[X]$ tales que $gr(f), gr(g) \leq n$ y $f(a_i) = g(a_i)$ para $i = 1, \ldots n + 1$. Entonces $f = g$.*

*Demostración.* El polinomio $f - g$ tiene grado menor o igual a $n$ y tiene $n + 1$ raíces distintas. Luego tiene que ser el polinomio cero. □

**Corolario 4.2.8.** *Sea $A$ un dominio de integridad infinito y sean $f, g \in A[X]$ tales que para todo $a \in A$ se verifica $f(a) = g(a)$. Entonces $f = g$.*

Este último corolario nos dice que si $A$ es un dominio de integridad infinito, la correspondencia entre polinomios y funciones polinómicas es biyectiva.

El anterior corolario se generaliza a varias indeterminadas:

**Teorema 4.2.9.** *Sea $A$ un dominio de integridad infinito y sea $f \in A[X_1, \ldots, X_n]$ tal que para cualesquiera $a_1, \ldots, a_n \in A$ se verifica $f(a_1, \ldots, a_n) = 0$. Entonces $f = 0$.*

*Demostración.* Inducción sobre $n$. □

**Corolario 4.2.10** (Principio de irrelevancia de desigualdades algebraicas)**.** *Sea $A$ un dominio de integridad infinito y sean $f, g, h \in A[X]$, $h \neq 0$ tales que para $a_1, \ldots, a_n \in A$, $h(a_1, \ldots, a_n) \neq 0 \Rightarrow f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$. Entonces $f = g$.*

*Demostración.* El polinomio $(f - g)h$ se anula sobre todos los $a_1, \ldots, a_n \in A$. Luego $(f - g)h = 0$. Como $A[X_1, \ldots, X_n]$ es un dominio de integridad y $h \neq 0$, necesariamente $f - g = 0$. □

El principio de irrelevancia de desigualdades algebraicas se llama también *propiedad de densidad*, por su interpretación en geometría algebraica.

## 4.3. Factorización

Sea $K$ un cuerpo. El anillo $K[X]$ es un dominio euclídeo y por tanto también es un dominio de factorización única.Vamos ahora a estudiar la factorización de polinomios en ese anillo. En primer lugar caracterizamos los elementos invertibles:

**Lema 4.3.1.** *Las unidades de $K[X]$ son los polinomios constantes no nulos.*

El primer teorema proporciona algunos polinomios irreducibles:

**Teorema 4.3.2.** *Los polinomios de grado uno son irreducibles en $K[X]$.*
*Estos son los únicos irreducibles si y sólo si todo polinomio de $K[X]$ de grado positivo tiene una raíz en $K$.*

*Demostración.* El primer resultado se deduce del teorema del grado.

Supongamos que todo polinomio irreducible es de grado uno. El anillo $K[X]$ es un dominio de factorización única, por tanto todo polinomio $f$ no constante es divisible por un irreducible, así que existe un $b_1X - b_0$ con $b_1 \neq 0$ tal que $f = (b_1X - b_0)q$. Pero entonces $f(b_0/b_1) = 0$ y $f$ tiene una raíz $b_0/b_1 \in K$.

A la inversa, si todo polinomio no constante tiene una raíz en $K$, sea $f$ un polinomio irreducible y sea $a \in K$ tal que $f(a) = 0$. Por el teorema del resto $X - a$ divide a $f$. Como $f$ es irreducible, debe ser asociado a $X - a$ y por tanto es de grado uno. □

**Definición 4.3.3.** Un cuerpo en que todo polinomio no constante tiene una raíz se llama *algebraicamente cerrado*.

El llamado *teorema fundamental del álgebra* dice que el cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado. Este hecho fue conjeturado por D'Alembert y demostrado por primera vez por el gran Gauss en su tesis doctoral. Dicha demostración tenía una laguna, pero a lo largo de su vida Gauss proporcionó cinco demostraciones correctas distintas. Sin embargo todas esas demostraciones utilizan bastante maquinaria analítica (como es propio, porque la construcción de $\mathbb{C}$ se basa en $\mathbb{R}$ que es el objeto de estudio del análisis matemático). Desde un punto de vista puramente algebraico, el hecho de que $\mathbb{C}$ sea algebraicamente cerrado es relativamente poco importante. Es mas importante demostrar que todo cuerpo $K$ es un subcuerpo de otro cuerpo $\bar{K}$ algebraicamente cerrado.

La factorización de polinomios con coeficientes en un cuerpo algebraicamente cerrado (como $\mathbb{C}$) es muy sencilla: Todo polinomio no constante es un producto de polinomios de grado uno.

Sobre los números reales es casi igual de fácil: Todo polinomio no constante es un producto de polinomios irreducibles de grado uno y dos. Sobre el cuerpo $\mathbb{Q}$ de los números racionales la situación es muy diferente: Existen polinomios irreducibles de todos los grados y para un polinomio $f \in \mathbb{Q}[X]$ dado puede ser penoso hallar sus factores. El resto de esta sección y las dos siguientes van encaminadas a intentar factorizar polinomios en $\mathbb{Q}[X]$.

Vamos a establecer los teoremas en un contexto mas general: Sea $A$ un dominio de factorización única y sea $K$ su cuerpo de fracciones.

**Definición 4.3.4.** Para todo polinomio no nulo $f = a_nX^n + \cdots + a_0 \in A[X]$ llamamos *contenido de $f$* a $c(f) = \text{m. c. d.}(a_n, \ldots, a_0)$.

Un polinomio $f \in A[X]$ se llama *primitivo* si $c(f) = 1$.

**Lema 4.3.5.** *Todo polinomio $f \in A[X]$ se expresa como $f = c(f)f_1$ con $f_1$ primitivo.*

**Teorema 4.3.6** (Lema de Gauss)**.** *El producto de dos polinomios primitivos es primitivo.*

*Demostración.* Sean $f = a_nX^n + \cdots + a_0$, $g = b_mX^m + \cdots + b_0$ dos polinomios primitivos de $A[X]$. Sea $p \in A$ un primo de $A$ arbitrario. Como $f, g$ son primitivos, m. c. d.$(a_n, \ldots, a_0) = 1 =$ m. c. d.$(b_m, \ldots, b_0)$ y en cada uno de ellos existe por lo menos un coeficiente no divisible por $p$. Sean $a_i$ y $b_j$ los primeros coeficientes no divisibles por $p$, de forma que para todo $k > i$, $p$ divide a $a_k$ y para todo $l > j$, $p$ divide a $b_l$. En el polinomio producto $fg$ consideramos el coeficiente del término de grado $i + j$:

$$c_{i+j} = (a_{i+j}b_0 + \cdots + a_{i+1}b_{j-1}) + a_ib_j + (a_{i-1}b_{j+1} + \cdots + a_0b_{i+j}$$

Todos los términos del primer paréntesis (que puede ser vacío) son divisibles por $p$, como también lo son todos los términos del segundo paréntesis (que también puede ser vacío). Así que $c_{i+j} = q_1p + a_ib_j + q_2p$ con $q_1, q_2 \in A$. Si $p$ dividiese a $c_{i+j}$, necesariamente $p \mid a_ib_j$ y como $p$ es primo, dividiría a uno de los factores, lo cual es imposible. Luego $p$ no divide a $c_{i+j}$.

Hemos demostrado que para todo primo $p \in A$ existe un coeficiente del producto $h = fg$ que no es divisible por $p$. Luego el máximo común divisor de los coeficientes de $h$ es 1 y $h$ es primitivo. □

**Corolario 4.3.7.** *Para dos polinomios $f, g \in A[X]$, el contenido del producto es el producto de los contenidos, es decir $c(fg) = c(f)c(g)$.*

**Teorema 4.3.8.** *Sea $f \in A[X]$ primitivo. Entonces $f$ es irreducible en $A[X]$ si y sólo si es irreducible en $K[X]$.*

*Demostración.* Supongamos que $f = gh$ es una factorización de $f$ en $K[X]$. Multiplicando por un denominador común obtenemos $k = af = bg_1h_1$, donde $a, b \in A$ y los polinomios $g_1, h_1$ son primitivos. Por el lema de Gauss el producto $g_1h_1$ también es primitivo. Luego $a$ y $b$ son ambos contenidos del polinomio $k$, luego son asociados. Sea $b = ua$ con $u$ invertible. Sustituyendo y simplificando nos queda $f = (uf_1)g_1$ donde $uf_1, g_1 \in A[X]$ son primitivos y $gr(uf_1) = gr(f)$, $gr(g_1) = gr(g)$. Luego $f$ es factorizable en $A[X]$.

A la inversa, sea $f = gh$ una factorización en $A[X]$. Los polinomios $f, g$ no son constantes y tienen sus coeficientes en $K$, luego esa misma es una factorización en $K[X]$.

Hemos visto que $f$ es reducible en $A[X]$ si y sólo si es reducible en $K[X]$. El contrarrecíproco es el resultado buscado. □

**Corolario 4.3.9.** *Los elementos irreducibles en $A[X]$ son de uno de los siguientes tipos:*

1. *Polinomios de grado cero que son irreducibles en $A$*
2. *Polinomios primitivos que son irreducibles en $K[X]$.*

**Teorema 4.3.10.** *Sea $A$ un dominio de integridad. El anillo $A$ es un dominio de factorización única si y sólo si $A[X]$ es un dominio de factorización única.*

*Demostración.* En primer lugar supongamos que $A[X]$ es un dominio de factorización única. Los elementos de $A$ pertenecen a $A[X]$ y por tanto descomponen de manera única como producto de irreducibles en $A[X]$, necesariamente todos de grado cero. Por tanto todo $a \in A$ descompone de manera única como producto de irreducibles en $A$. Luego $A$ es un dominio de factorización única.

A la inversa sea $A$ un dominio de factorización única. Sea $f \in A[X]$ no cero. Descomponemos $f = c(f)f_1$ con $f_1$ primitivo. Descomponemos $c(f) = p_1 \ldots p_t$ en producto de irreducibles en $A$ y $f_1 = q_1 \ldots q_s$ en producto de primitivos irreducibles en $K[X]$. Entonces $f = p_1 \ldots p_tq_1 \ldots q_s$ es una descomposición de $f$ en producto de irreducibles en $A[X]$.

Sea ahora $p$ un irreducible en $A[X]$ y sean $f, g \in A[X]$ tales que $p$ divide al producto $fg$.

Si $gr(p) = 0$, entonces $p$ es irreducible y primo en $A$ y $p$ divide al contenido $c(fg) = c(f)c(g)$. Luego $p$ divide a $c(f)$ (en cuyo caso divide a $f$) o divide a $c(g)$ (en cuyo caso divide a $g$. Luego $p$ es primo.

Si $gr(p) > 0$, entonces $p$ es un polinomio primitivo irreducible y por tanto primo en $K[X]$. Luego $p$ divide a $f$ o a $g$ en $K[X]$. Sea $q$ un polinomio en $K[X]$ tal que $f = pq$. Extrayendo contenidos, vemos que $q$ pertenece a $A[X]$ y por tanto $p$ divide a $f$ en $A[X]$. Luego $p$ es primo en $A[X]$.

Hemos demostrado que todo polinomio de $A[X]$ descompone como producto de irreducibles y que todo irreducible es primo. Luego $A[X]$ es un dominio de factorización única. □

**Corolario 4.3.11.** *Sea $A$ un dominio de integridad. Entonces $A$ es un dominio de factorización única si y sólo si $A[X_1, \ldots, X_n]$ es un dominio de factorización única.*

**Corolario 4.3.12.** *Sea $K$ un cuerpo. El anillo $K[X_1, \ldots, X_n]$ es un dominio de factorización única.*

## 4.4. Criterios de irreducibilidad

En esta sección $A$ es un dominio de factorización única y $K$ es su cuerpo de fracciones, salvo mención expresa en contrario.

La factorización en el anillo de polinomios $A[X]$ presenta dos problemas prácticos relacionados entre sí:

1. Dado un polinomio $f \in A[X]$ determinar si es reducible o irreducible
2. Si $f$ es reducible, factorizarlo en irreducibles.

Para el primer caso muchas veces basta tener criterios suficientes (es decir, que si un polinomio satisface el criterio, es irreducible. Si no lo satisface no podemos decir nada). Evidentemente, una solución general del segundo punto incluiría criterios necesarios y suficientes para que un polinomio dado sea irreducible.

Empezamos determinando los factores de grado uno:

**Proposición 4.4.1.** *Sean $f = a_n X^n + \cdots + a_0$, $g = b_m X + b_0 \in A[X]$ con $a_n, b_m \neq 0$. Si $g$ divide a $f$, necesariamente $b_m$ divide a $a_n$ y $b_0$ divide a $a_0$*

*Demostración.* Sea $h = c_k X^k + \cdots + c_0 \in A[X]$ tales que $f = gh$. Entonces el coeficiente líder del producto es $a_n = b_m c_k$ y el término independiente es $a_0 = b_0 c_0$ □

**Corolario 4.4.2** (Regla de Ruffini)**.** *Sea $f = a_n X^n + \cdots + a_0$ y sea $a/b \in K$ tal que* m. c. d.$(a, b) = 1$ *y $f(a/b) = 0$. Entonces $a$ divide a $a_0$ y $b$ divide a $a_n$.*

La regla de Ruffini la describió ya Newton en su libro *Arithmetica Universalis* (publicado en 1707, cincuenta y ocho años antes del nacimiento de Ruffini), para determinar las raíces racionales y enteras de polinomios con coeficientes enteros. El corolario anterior permite usarla para hallar las raíces de polinomios con coeficientes en cualquier dominio de fatorización única.

*Ejemplo* 4.4.3. Sea $f = X^4 + 4 \in \mathbb{Z}[X]$. Cualquier raíz racional suya debe ser de la forma $a/b$ con $b \mid 1$ y $a \mid 4$. Luego las posibles raíces racionales de $f$ son $1, -1, 2, -2, 4, -4$. Un cálculo rápido muestra que ninguno de estos números es raíz de $f$, luego el polinomio $f$ no tiene raíces en $\mathbb{Q}$.

*Ejemplo* 4.4.4. Sea ahora $f = X^4 + 4 \in \mathbb{J}[X]$. Los divisores de 4 son ahora $1, 1+i, 2, 2+2i, 4$ y sus asociados (todos los productos por las unidades $\pm 1, \pm i$). Un nuevo cálculo muestra que $f(1+i) = f(1-i) = f(-1+i) = f(-1-i) = 0$, luego $f$ tiene cuatro raíces en $\mathbb{J}$ y factoriza como

$$X^4 + 4 = (X - (i+i))(X - (i-i))(X - (-i+i))(X - (-i-i))$$

Un criterio de aplicación muy rápida es debido a un discípulo de Gauss:

**Teorema 4.4.5** (Criterio de Eisenstein)**.** *Sea $f = a_n X^n + \cdots + a_0$ un polinomio primitivo y sea $p \in A$ un primo tal que $p \nmid a_n$, $p \mid a_i$ para $i = n-1, \ldots, a_0$ y $p^2 \nmid a_0$. Entonces $f$ es irreducible en $A[X]$.*

*Demostración.* Supongamos que $f$ es reducible, $f = gh$ con $g = b_m X^m + \cdots + b_0$ y $h = c_r X^r + \cdots + c_0$ con $m, r \geq 1$ y $n = m+r$. Como $p$ no divide a $a_n = b_m c_r$, necesariamente $p \nmid b_m$ y $p \nmid c_r$. Como $p$ divide a $a_0 = b_0 c_0$, $p$ debe dividir a uno de los factores, sea $p \mid b_0$. Entonces $p$ no divide a $c_0$ porque $p^2 \nmid a_0 = b_0 c_0$. Sea $i$ tal que $p \nmid b_i$ pero $p \mid b_j$ para todo $j < i$. El coeficiente en $f$ del término de grado $i$ es $a_i = b_i c_0 + (b_{i-1} c_1 + \cdots + b_0 c_i)$. Todos los términos del paréntesis son divisibles por $p$ y $p \nmid b_i c_0$, luego $p \nmid a_i$. Pero $i \leq m < n$, luego por la hipótesis $p \mid a_i$, contradicción. □

*Ejemplo* 4.4.6. Sea $f = 2X^5 - 6X^3 + 9X^2 - 15 \in \mathbb{Z}[X]$. El polinomio $f$ es primitivo porque m. c. d.$(2, -6, 9, -15) = 1$. El primo 3 divide a todos los coeficientes menos al líder, y $3^2 = 9$ no divide al término independiente, luego $f$ es irreducible en $\mathbb{Z}[X]$.

*Ejemplo* 4.4.7. Sea $f = Y^3 + X^2 Y^2 + XY + X \in K[X, Y]$ con $K$ un cuerpo arbitrario. Como $K[X, Y] = A[Y]$ con $A = K[X]$ dominio euclídeo, aplicando el criterio de Eisenstein con el primo $X \in A[X]$ vemos que $f$ es irreducible en $K[X, Y]$.

A veces el polinomio dado no satisface las condiciones del criterio de Eisenstein pero un transformado sencillo sí las satisface. Del siguiente lema podemos deducir entonces la irreducibildad del polinomio original:

**Lema 4.4.8.** *Sea $A$ un dominio de integridad y sea $f \in A[X]$. Sea $a \in A$ arbitrario y sea $f_a(X) = f(X + a)$. Entonces $f$ descompone como $f = gh$ con $gr(g), gr(h) > 0$ si y sólo si $f_a = g_a h_a$. En este caso $gr(g_a) = gr(g) > 0$ y $gr(h_a) = gr(h) > 0$.*

*Demostración.* Cálculo trivial. □

**Corolario 4.4.9.** *Sea $A$ un dominio de factorización única y sea $f \in A[X]$ primitivo. Sea $a \in A$ arbitrario tal que $f_a$ sea primitivo. Entonces $f$ es irreducible si y sólo si $f_a$ es irreducible*

*Ejemplo* 4.4.10. Sea $f = X^4 + 1 \in \mathbb{Z}[X]$. No podemos aplicar directamente el criterio de Eisenstein a $f$. Pero

$$f_1 = f(X + 1) = (X + 1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$$

satisface las condiciones del criterio de Eisenstein con $p = 2$. Luego $f_1$ es irreducible en $\mathbb{Z}[X]$ y por tanto también lo es $f$.

*Ejemplo* 4.4.11. (Este ejemplo se remonta a Gauss). Sea $p \in \mathbb{Z}$ un primo. El polinomio

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$$

se llama *p-ésimo polinomio ciclotómico*. Vamos a comprobar que $\Phi_p$ es irreducible en $\mathbb{Z}[X]$ (y por tanto en $\mathbb{Q}[X]$): Calculamos el desarrollo de $f = \Phi_p(X + 1)$:

$$f = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{(\sum_{i=0}^{p} \binom{p}{i} X^i) - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}$$

Ahora $p$ no divide al coeficiente líder $\binom{p}{p} = 1$, $p$ divide a $\binom{p}{i}$ para $i = p - 1, \ldots 1$ y $p^2$ no divide al término independiente $\binom{p}{1} = p$. Luego $f$ es irreducible en $\mathbb{Z}[X]$ y por tanto también lo es $\Phi_p$.

A veces se utiliza otra transformación del polinomio:

**Definición 4.4.12.** Sea $f = a_n X^n + a_{n-1} X^{n-1} \cdots + a_1 X + a_0 \in A[X]$ un polinomio con $a_n, a_0 \neq 0$. Se llama *polinomio reciproco de $f$* al polinomio

$$f_{rec} = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n = X^n f\left(\frac{1}{X}\right)$$

**Lema 4.4.13.** *Sea $f \in A[X]$ primitivo. Entonces $f$ es irreducible en $A[X]$ si y sólo si $f_{rec}$ es irreducible.*

*Demostración.* Los coeficientes de $f_{rec}$ son los mismos que los de $f$, luego $f_{rec}$ es primitivo. Sea ahora $f = gh$ con $m = gr(g), r = gr(h)$ y $n = gr(f) = m + r$. Entonces

$$f_{rec} = X^n f\left(\frac{1}{X}\right) = X^m X^r g\left(\frac{1}{X}\right) h\left(\frac{1}{X}\right) = g_{rec} h_{rec}$$

□

*Ejemplo* 4.4.14. Sea $f = 6X^4 + 9X^3 - 3X^2 + 1 \in \mathbb{Z}[X]$. El primo $p = 3$ divide a todos los coeficientes menos al término independiente y $3^2 = 9$ no divide al coeficiente líder, luego $f$ es irreducible.

Cuando se puede aplicar, el criterio de Eisenstein es una prueba muy rápida de irreducibilidad. Pero son muy pocos los polinomios a los que es aplicable. Existe otro criterio que se puede aplicar a mas polinomios y aunque falle, los resultados que se obtienen en su aplicación son útiles para intentar posteriormente la factorización del polinomio.

Todo homomorfismo de anillos $\sigma : A \to B$ define un homomorfismo $A[X] \to B[X]$ que también se denota por $\sigma$ de la siguiente forma: Sea $f = a_n X^n + \cdots + a_0$. Entonces $\sigma(f) = \sigma(a_n)X^n + \cdots + \sigma(a_0)$.

**Proposición 4.4.15.** *Sean $A, B$ dos dominios de integridad con cuerpos de fracciones respectivos $K$ y $L$. Sea $\sigma : A \to B$ un homomorfismo de anillos y sea $f \in A[X]$ un polinomio tal que $gr(\sigma(f)) = gr(f)$. Si $f = gh$, entonces $\sigma(f) = \sigma(g)\sigma(h)$ con $gr(\sigma(g)) = gr(g)$ y $gr(\sigma(h)) = gr(h)$.*

**Corolario 4.4.16** (Criterio de reducción)**.** *Si $\sigma(f)$ es irreducible en $L[X]$, entonces $f$ es irreducible en $K[X]$.*

Usualmente este criterio se aplica con $A = \mathbb{Z}$, $K = \mathbb{Q}$, $B = L = \mathbb{Z}_p$ y $\sigma : \mathbb{Z} \to \mathbb{Z}_p$ la proyección canónica que lleva cada entero $n$ en su clase módulo $p$, o sea $\sigma(n) = \bar{n} = [n]_p$. En este caso se suele denotar $\sigma(f) = \bar{f}$.

*Ejemplo* 4.4.17. Sea $p \in \mathbb{Z}$ un número primo. El polinomio $X^p - X - 1 \in \mathbb{Z}_p[X]$ es irreducible, luego $f = X^p - X - 1$ es irreducible en $\mathbb{Z}[X]$.

De la misma forma el polinomio $f = X^5 - 5X^4 - 6X - 1 \in \mathbb{Z}[X]$ es irreducible en $\mathbb{Z}[X]$ (porque módulo 5, $\sigma(f) = X^5 - X - 1 \in \mathbb{Z}_5[X]$).

El inverso del criterio de irreducibilidad es falso:

*Ejemplo* 4.4.18. El polinomio $f = X^3 - 3 \in \mathbb{Z}[X]$ es irreducible por el criterio de Eisenstein, pero módulo 2 $\sigma(f) = (X + 1)(X^2 + X + 1)$, luego puede ocurrir perfectamente que $f$ sea irreducible y $\sigma(f)$ no lo sea.

La proposición 4.4.15 puede usarse combinando la información sobre los factores de $f$ que se obtiene utilizando diversos primos:

*Ejemplo* 4.4.19. Sea $f = X^5 - 6X^4 + 5X^2 - X + 2$. Módulo 2 tenemos $\bar{f} = X^5 + X^2 + X = X(X^4 + X + 1)$ con ambos factores irreducibles. Si $f$ es reducible, debe factorizar como producto de un polinomio de grado 1 por otro de grado 4.

Reduciendo módulo 3 queda $\bar{f} = X^5 - X^2 - X - 1 = (X^2 + 1)(X^3 - X - 1)$ con ambos factores irreducibles, así que si $f$ fuese reducible debería factorizar como producto de un polinomio de grado 2 por otro de grado 3. Luego las factorizaciones módulo 2 y tres son incompatibles y $f$ es irreducible en $\mathbb{Z}[X]$.

*Ejemplo* 4.4.20. Sea $f = X^4 - 22X^2 + 1 \in \mathbb{Z}[X]$. Reduciendo módulo 2 obtenemos $\bar{f} = X^4 + 1 = (X + 1)^4$, lo que no nos da información interesante. Módulo 3 es $\bar{f} = X^4 + 2X^2 + 1 = (X^2 + 1)^2$, luego si $f$ factoriza en $\mathbb{Z}[X]$, debe hacerlo como producto de dos polinomios de grado 2, $f = gh$. Además los términos constantes de $g$ y $h$ deben ser divisores de 1 y congruentes con 1 módulo 3, luego ambos valen 1.

Supongamos que $f = (X^2 + aX + 1)(X^2 + bX + 1) = X^4 + (a + b)X^3 + (ab + 2)X^2 + (a + b)X + 1)$. Comparando coeficientes debe ser $a + b = 0$ y $ab + 2 = -22$, así que $b = -a$ y $a^2 = 24$. Esta última ecuación no tiene solución con $a$ entero, luego la factorización es imposible y $f$ es irreducible.

## 4.5. Factorización en un número finito de pasos

Si el polinomio dado $f$ es reducible, el problema es determinar los factores de $f$ en un número finito de pasos (y en un tiempo razonable). En el libro *Arithmetica Universalis* citado antes, Newton describe cómo hallar los factores cuadráticos de un polinomio con coeficentes enteros. Esta es la traslación de dicho método a dominios de factorización única:

Sea $A$ un dominio de factorización única con un número finito de unidades y sea $f = gh \in A[X]$ con

$$f = a_n X^n + \cdots + a_0$$
$$g = b_2 X^2 + b_1 X + b_0$$

Entonces $b_2$ divide a $a_n$, $b_0$ divide a $a_0$ y $g(1) = b_2 + b_1 + b_0$ divide a $f(1) = a_n + \cdots + a_0$. Estas condiciones limitan a un número finito las posibilidades para $b_2, b_0$ y $b_1$. Para cada una de las ternas $(b_2, b_1, b_0)$ posibles construimos el polinomio $g$ y probamos a dividir $f$ por $g$. Así se determinan todos los factores cuadráticos de $f$.

Para limitar aún mas el conjunto de posibles divisores se utiliza la condición de que $g(-1) = b_2 - b_1 + b_0$ divide a la suma alternada $(-1)^n f(-1) = a_n - a_{n-1} + \cdots \pm 1$. Además podemos utilizar la información que hayamos obtenido reduciendo diversos primos.

*Ejemplo* 4.5.1. Sea $f = X^4 + 4 \in \mathbb{Z}[X]$. Usando la regla de Ruffini vemos que $f$ no tiene raíces enteras. Sea $g = b_2 X^2 + b_1 X + b_0$ un factor de $f$ Como $f$ es mónico, podemos tomar $b_2 = 1$. Reduciendo módulo 2 tenemos $\bar{f} = X^4 = \bar{g}\bar{h}$, luego los términos constantes de $g$ y del cociente $h$ son pares. Como su producto es 4, necesariamente $b_0 = \pm 2$. Módulo 3 tenemos $\bar{f} = X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1)$, luego $b_0 \equiv -1$ (mód 3), lo que nos deja $b_0 = 2$.

Ahora $1 + b_1 + 2 = b_1 + 3$ divide a $f(1) = 5$, lo que se verifica sólo para $b_1 = -8, -4, -2, 2$ y $1 - b_1 + 2 = -b_1 + 3$ divide a $f(-1) = 5$, lo que reduce las posibilidades a $b_1 = -2, 2$. Así que los únicos divisores de grados dos posibles son $g_1 = X^2 + 2X + 2$ y $g_2 = X^2 - 2X + 2$. Un cálculo fácil muestra que $f = g_1 g_2$.

El anterior método de Newton fué extendido en 1793 por Friedrich von Schubert, quien mostró cómo hallar todos los factores de grado $m$ en un número finito de pasos. Unos 90 años después Leopoldo Kronecker descubrió independientemente el método de Schubert. Desgraciadamente el método es muy ineficiente cuando $gr(f) \geq 5$ y es mejor utilizar métodos de reducción (descritos en [3] y [8]) . El método de Kronecker se describe en la siguiente demostración:

**Teorema 4.5.2** (Kronecker)**.** *Sea $A$ un dominio de factorización única con un número finito de unidades. Entonces es posible descomponer cualquier polinomio $f \in A[X]$ en factores irreducibles en un número finito de pasos.*

*Demostración.* Dado un polinomio $f \in A[X]$, el método consiste en determinar para cada $m < n/2$ un conjunto finito $\mathcal{S}$ de polinomios entre los que están todos los divisores de $f$ de grado menor o igual a $m$. Posteriormente se prueba a dividir $f$ por cada uno de los polinomios del conjunto $\mathcal{S}$ y así determinamos los divisores de grado menor o igual a $m$.

Si $f = gh$, para todo $a \in A$ se verifica que $f(a) = g(a)h(a)$, luego $g(a)$ divide a $f(a)$. Sean $a_0, \ldots, a_m \in A$ elementos distintos. Para cada $i = 0, \ldots, m$ sea $D_i$ el conjunto de divisores de $f(a_i)$. Para cada sucesión $\mathbf{b} = (b_0, \ldots, b_m) \in D_0 \times \cdots \times D_m$ sea $g_{\mathbf{b}}$ el único polinomio de grado menor o igual a $m$ que verifica $g_{\mathbf{b}}(a_i) = b_i$, $i = 0, \ldots m$ (El polinomio $g_{\mathbf{b}}$ es el *polinomio de interpolación*, que se obtiene por uno de los métodos de Newton o de Lagrange). El conjunto $\mathcal{S} = \{g_{\mathbf{b}} \mid \mathbf{b} \in D_0 \times \cdots \times D_m\}$ es finito y contiene a todos los divisores de $f$ de grado menor o igual a $m$. □

En la práctica se achica bastante el conjunto $\mathcal{S}$ utilizando la información que hayamos obtenido por reducción módulo diversos primos, igual que hicimos antes en el ejemplo 4.5.1

*Ejemplo* 4.5.3. Sea $f = X^6 - X^5 - X^4 + X^3 + X^2 - X - 1 \in \mathbb{Z}[X]$. Queremos encontrar los factores de grado menor o igual a tres, así que evaluamos $f$ en cuatro (=3+1) puntos distintos. Elegimos los puntos $-2, -1, 0, 1$. Evaluamos: $f(-2) = 77$, $f(-1) = 1$, $f(0) = -1$, $f(1) = -1$. El conjunto $D_0 \times \cdots \times D_3 = \{\pm 1, \pm 7, \pm 11, \pm 77\} \times \{\pm 1\} \times \{\pm 1\} \times \{\pm 1\}$,así que en total hay que calcular $8 \cdot 2 \cdot 2 \cdot 2 = 64$ polinomios. Usando los interpoladores de Lagrange, estos polinomios son

$$\begin{aligned} f_b &= b_0 \frac{(X+1)X(X-1)}{(-2+1)(-2)(-2-1)} + b_1 \frac{(X+2)X(X-1)}{(-1+2)(-1)(-1-1)} \\ &+ b_2 \frac{(X+2)(X+1)(X-1)}{(0+2)(0+1)(0-1)} + b_3 \frac{(X+2)(X+1)X}{(1+2)(1+1)(1)} \\ &= b_0 \frac{X^3 - X}{-6} + b_1 \frac{X^3 + X^2 - 2X}{2} + b_2 \frac{X^3 + 2X^2 - X - 2}{-2} + b_3 \frac{X^3 + 3X^2 + 2X}{6} \end{aligned}$$

Calculamos los 64 polinomios. La mitad de ellos no tiene coeficientes enteros y los restantes se agrupan de dos en dos salvo el signo. Eligiendo uno de cada par de opuestos, nos quedan dieciseis polinomios:

| $b_0$ | $b_1$ | $b_2$ | $b_3$ | $g_b$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | $1$ |
| 7 | 1 | 1 | 1 | $-X^3 + X + 1$ |
| $-11$ | 1 | 1 | 1 | $2X^3 - 2X + 1$ |
| $-77$ | 1 | 1 | 1 | $13X^3 - 13X + 1$ |
| 1 | $-1$ | 1 | 1 | $-X^3 - X^2 + 2X + 1$ |
| 7 | $-1$ | 1 | 1 | $-2X^3 - X^2 + 3X + 1$ |
| $-11$ | $-1$ | 1 | 1 | $X^3 - X^2 + 1$ |
| $-77$ | $-1$ | 1 | 1 | $12X^3 - X^2 - 11X + 1$ |
| 1 | 1 | $-1$ | 1 | $X^3 + 2X^2 - X - 1$ |
| 7 | 1 | $-1$ | 1 | $2X^2 - 1$ |
| $-11$ | 1 | $-1$ | 1 | $3X^3 + 2X^2 - 3X - 1$ |
| $-77$ | 1 | $-1$ | 1 | $14X^3 + 2X^2 - 14X - 1$ |
| 1 | $-1$ | $-1$ | 1 | $X^2 + X - 1$ |
| 7 | $-1$ | $-1$ | 1 | $-X^3 + X^2 + 2X - 1$ |
| $-11$ | $-1$ | $-1$ | 1 | $2X^3 + X^2 - X - 1$ |
| $-77$ | $-1$ | $-1$ | 1 | $13X^3 + X^2 - 12X - 1$ |

El polinomio $f$ dado es mónico, así que buscamos factores mónicos. Repasando la lista anterior nos queda que sus posibles divisores mónicos de grado menor o igual que tres son

$$\begin{aligned} &1 \\ &X^3 - X - 1 \\ &X^3 + X^2 - 2X + 1 \\ &X^3 - X^2 + 1 \\ &X^3 + 2X^2 - X - 1 \\ &X^2 + X - 1 \\ &X^3 - X^2 - 2X + 1 \end{aligned}$$

El 1 es trivial. Probando a dividir sucesivamente por cada uno de los otros obtenemos la factorización

$$f = (X^3 - X - 1)(X^3 - X^2 + 1)$$

y los dos factores son irreducibles (son de grado 3 y no tienen raíces enteras).

## 4.6. Polinomios simétricos

Sea $A$ un anillo conmutativo y sean $X_1, \dots, X_n$ indeterminadas. Sea $S_n$ el grupo simétrico sobre $\{1, \dots, n\}$. Para toda permutación $\sigma \in S_n$ definimos

$$\sigma \cdot f(X_1, \dots, X_n) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

Por ejemplo, sea $f = X_1^2 X_2 - X_3$ y sean $\rho = (1\ 3)$, $\sigma = (1\ 2\ 3)$. Entonces $\rho \cdot f = X_3^2 X_2 - X_1$ y $\sigma \cdot f = X_2^2 X_3 - X_1$.

**Definición 4.6.1.** Un polinomio $f \in A[X_1, \dots, X_n]$ se llama *simétrico* si para toda permutación $\sigma \in S_n$ se verifica $\sigma \cdot f = f$.

**Lema 4.6.2.** *El conjunto de polinomios simétricos es un subanillo de $A[X_1, \dots, X_n]$ que contiene al anillo $A$.*

Sea $Y$ otra indeterminada. Formamos el polinomio

$$\begin{aligned} F(Y, X_1, \dots, X_n) &= (Y - X_1) \dots (Y - X_n) \\ &= Y^n - s_1 Y^{n-1} + \dots + (-1)^n s_n \end{aligned}$$

con coeficientes en $A[X_1, \dots, X_n]$. Los polinomios coeficientes $s_1 = X_1 + \dots + X_n, \dots, s_n = X_1 \dots X_n$ son polinomios simétricos, y se llaman *polinomios simétricos elementales*. Obsérvese que el polinomio $s_i$ es homogéneo de grado $i$.

**Definición 4.6.3.** Sea $a_e X_1^{e_1} \dots X_n^{e_n}$ un monomio no nulo. Se llama *peso* del monomio al entero $e_1 + 2e_2 + \dots + ne_n$.

Sea $g \in A[X_1, \dots, X_n]$. El *peso de $g$* es el mayor de los pesos de los monomios no nulos de $g$.

**Teorema 4.6.4** (Teorema fundamental de los polinomios simétricos)**.** *Sea $A$ un dominio de integridad y sea $f \in A[X_1, \dots, X_n]$ un polinomio simétrico de grado $d$. Entonces existe un único polinomio $g \in A[X_1, \dots, X_n]$ de peso menor o igual a $d$ tal que*

$$f(X_1, \dots, X_n) = g(s_1, \dots, s_n)$$

*Demostración.* Inducción sobre $n$ y $d$.

Si $n = 1$, sólo hay una indeterminada, así que $s_1 = X_1$ y $g = f$ verifica las condiciones (el peso de $f$ es igual al grado).

Sea ahora $n > 1$ y supongamos el teorema cierto para $n - 1$ indeterminadas. Si $d = 0$, el polinomio $f$ es constante. Tomando $g = f$ se verifica el teorema (en este caso, el grado y el peso de $f$ son ambos iguales a cero).

Finalmente sean $n > 1$, $d > 0$ y suponemos el teorema cierto para todo polinomio simétrico en $n$ indeterminadas de grado menor que $d$. En el anterior polinomio $F$ sustituimos $X_n = 0$. Obtenemos

$$\begin{aligned} F(Y, X_1, \dots, X_{n-1}, 0) &= (Y - X_1) \dots (Y - X_{n-1}) Y \\ &= Y^n - (s_1)_0 Y^{n-1} + \dots + (-1)^{n-1} (s_{n-1})_0 Y \end{aligned}$$

donde $(s_i)_0$ se obtiene sustituyendo $X_n = 0$ en $s_i$.

Es inmediato que $(s_1)_0, \dots, (s_{n-1})_0$ son precisamente los polinomios simétricos elementales en $X_1, \dots, X_{n-1}$.

El polinomio $f(X_1, \ldots, X_{n-1}, 0) \in A[X_1, \ldots, X_{n-1}]$ es simétrico. Por la hipótesis de inducción sobre $n$, existe un polinomio $g_1 \in A[X_1, \ldots, X_{n-1}]$ de peso menor o igual a $d$ tal que $f(X_1, \ldots, X_{n-1}, 0) = g_1((s_1)_0, \ldots, (s_{n-1})_0)$. El polinomio

$$f_1(X_1, \ldots, X_n) = f(X_1, \ldots, X_n) - g_1(s_1, \ldots, s_{n-1})$$

es simétrico y tiene grado menor o igual a $d$. Además $f_1(X_1, \ldots, X_{n-1}, 0) = 0$, luego $f_1$ es divisible por $X_n$. Como es simétrico, también es divisible por $X_1, \ldots, X_{n-1}$. Como estos factores son primos relativos, su producto divide a $f_1$. Luego $f_1 = s_n f_2(X_1, \ldots, X_n)$ con un polinomio $f_2 \in A[X_1, \ldots, X_n]$ que es simétrico y de grado estrictamente menor que $d$. Por la inducción sobre $d$, existe un $g_2 \in A[X_1, \ldots, X_n]$ de peso menor o igual a $d - n$ tal que

$$f_2(X_1, \ldots, X_n) = g_2(s_1, \ldots, s_n)$$

Sustituyendo obtenemos

$$f(X_1, \ldots, X_n) = g_1(s_1, \ldots, s_{n-1}) + s_n g_2(s_1, \ldots, s_n)$$

y cada término del miembro de la derecha tiene un peso menor o igual a $d$.

La unicidad se deduce del próximo teorema. □

**Teorema 4.6.5.** *Sea $g \in A[X_1, \ldots, X_n]$. Entonces $g(s_1, \ldots, s_n) = 0$ si y sólo si $g(X_1, \ldots, X_n) = 0$.*

*Demostración.* Inducción sobre $n$. Si $n = 1$ el resultado es trivial.

Sea ahora $n > 1$ y suponemos el resultado cierto para $n - 1$ indeterminadas. Sea $g \in A[X_1, \ldots, X_n]$ no nulo de grado mínimo tal que $g(s_1, \ldots, s_n) = 0$. Escribimos $g$ como un polinomio en $X_n$ con coeficientes en $X_1, \ldots, X_{n-1}$:

$$g = g_0 + \cdots + g_d \cdot X_n^d$$

Sustituyendo $X_i$ por $s_i$ en el polinomio $g$ tenemos

$$0 = g_0(s_1, \ldots, s_{n-1}) + \ldots g_d(s_1 \ldots, s_{n-1}) s_n^d$$

Sustituyendo ahora $X_n = 0$ obtenemos

$$0 = g_0((s_1)_0, \ldots, (s_{n-1})_0)$$

Pero los $(s_i)_0$ son los polinomios simétricos elementales en $X_1, \ldots, X_{n-1}$. Por inducción $g_0(X_1, \ldots, X_{n-1}) = 0$.

Ya que $g_0 = 0$ podemos escribir $g = f \cdot X_n$ con $f \in A[X_1, \ldots, X_n]$ y por tanto $f(s_1, \ldots, s_n)s_n = 0$, luego $f(s_1, \ldots, s_n) = 0$ y $f$ es de grado estrictamente menor que $g$, lo cual es imposible. □

*Ejemplo* 4.6.6. Sea $f = (X_1 + X_2)(X_1 + X_3)(X_2 + X_3) \in \mathbb{Z}[X_1, , X_2, X_3]$. Es fácil comprobar que $f$ es un polinomio simétrico homogéneo de grado 3. Queremos encontrar un polinomio $g \in \mathbb{Z}[X_1, X_2, X_3]$ de peso menor o igual a 3 tal que $f = g(s_1, s_2, s_3)$. Para ello aplicamos la construcción de la demostración:

1. $f(X_1, 0, 0) = 0$, luego $g_1 = 0$.
2. $f(X_1, X_2, 0) = (X_1 + X_2)X_1X_2$. El resto del proceso de la demostración es trivial: $f(X_1, X_2, 0) = g((s_1)_0, (s_2)_0) = (s_1)_0(s_2)_0$.
3. La demostración construye ahora el polinomio

$$\begin{aligned}
&f_1(X_1, X_2, X_3) = f(X_1, X_2, X_3) - g(s_1, s_2)\\
&= (X_1 + X_2)(X_1 + X_3)(X_2 + X_3)\\
&- (X_1 + X_2 + X_3)(X_1X_2 + X_1X_3 + X_2X_3)\\
&= (X_1^2X_2 + X_1^2X_3 + X_1X_2^2 + X_1X_3^3 + X_2^2X_3 + X_2X_3^2 + 2X_1X_2X_3)\\
&- (X_1^2X_2 + X_1^2X_3 + X_1X_2^2 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2 + 3X_1X_2X_3)\\
&= -X_1X_2X_3
\end{aligned}$$

luego $f(X_1, X_2, X_3) = f_1(X_1, X_2, X_3) + X_1X_2X_3 = s_1s_2 - s_3$.

Para escribir los polinomios simétricos se ha desarrollado una notación especial: Llamamos $\sum X_1^{i_1} \dots X_n^{i_n}$ a la suma de todos los monomios distintos que se obtienen al aplicar todas las permutaciones de $S_n$ al monomio $X_1^{i_1} \dots X_n^{i_n}$. Por ejemplo si $n = 3$,

$$\sum X_1^3 = X_1^3 + X_2^3 + X_3^3$$

$$\sum X_1^2X_2 = X_1^2X_2 + X_1^2X_3 + X_2^2X_1 + X_2^2X_3 + X_3^2X_2 + X_3^2X_1$$

. Un polinomio simétrico general es una combinación lineal de términos de la forma $\sum X_1^{i_1} \dots X_n^{i_n}$ con coeficientes en $A$.

*Ejemplo* 4.6.7. Sea $f = \sum X_1^2X_2$ con $n = 3$. Calculamos $f(X_1, X_2, 0) = X_1^2X_2 + X_2^2X_1 = X_1X_2(X_1 + X_2) = (s_2)_0(s_1)_0$.

Ahora $f_1 = f - s_2s_1 = \sum X_1^2X_2 - (\sum X_1X_2)(\sum X_1) = -3X_1X_2X_3$. Luego $\sum X_1^2X_3 = s_1s_2 - 3s_3$.

*Ejemplo* 4.6.8. Seguimos tomando $n = 3$. Sea $f = \sum X_1^3$.

Entonces $f(X_1, 0, 0) = X_1^3 = (s_1)_{00}^3$.

El siguiente paso calcula $f(X_1, X_2, 0) - (s_1)_0^3 = -3(s_1)_0(s_2)_0$.

Luego $f(X_1, X_2, 0) = (s_1)_0^3 - 3(s_1)_0(s_2)_0$.

Finalmente calculamos $f_1(X_1, X_2, X_3) = f - (s_1^3 - 3s_1s_2) = 3X_1X_2X_3$,

así que $f = s_1^3 - 3s_1s_2 + 3s_3$.

*Ejemplo* 4.6.9. Sea $\Delta = \prod_{i<j}(X_i - X_j)$. El polinomio $d = \Delta^2$ es simétrico. Vamos a expresarlo en función de los polinomios simétricos elementales para $n = 3$.

1. En primer lugar $d(X_1, 0, 0) = ((X_1 - 0)((X_1 - 0)(0 - 0))^2 = 0$.
2. Ahora $d(X_1, X_2, 0) = ((X_1 - X_2)X_1X_2)^2$. Luego $d(X_1, X_2) = s_2^2 \cdot f_1$ con $f_1(X_1, X_2) = (X_1 - X_2)^2$.
   $f_1(X_1, 0) = X_1^2$. Entonces
   $$f_1(X_1, X_2) - (s_1)_0^2 = (X_1 - X_2)^2 - (X_1 + X_2)^2 = -4X_1X_2$$
   y por tanto $f_1 = (s_1)_0^2 - 4(s_2)_0$.
3. Finalmente tenemos
   $$\begin{aligned} g_1(X_1, X_2, X_3) &= d(X_1, X_2, X_3) - s_2^2(s_1^2 - 4s_2) \\ &= s_3 \cdot f_2 \end{aligned}$$
   con $f_2 = 6\sum X_1^2X_2 - 4\sum X_1^3 + 3X_1X_2X_3$. Por los dos ejemplos anteriores,
   $$\begin{aligned} d &= s_1^2s_2^2 - 4s_2^3 + s_3(6(s_1s_2 - 3s_3) - 4(s_1^3 - 3s_1s_2 + 3s_3) + 3s_3) \\ &= s_1^2s_2^2 - 4s_2^3 - 4s_1^3s_3 + 18s_1s_2s_3 - 27s_3^2 \end{aligned}$$

Existen otros tres métodos para expresar un polinomio simétrico en función de los simétricos elementales. Quizá el mas útil sea el *método de coeficientes indeterminados*: Descomponemos el polinomio simétrico dado en suma de polinomios simétricos homogéneos y expresamos cada uno de estos en función de los polinomios simétricos elementales. Para ello, expresamos cada uno de los polinomios homogéneos de grado $d$ como suma con coeficientes indeterminados de todos los $k$ monomios posibles en los $s_i$ de peso $d$. Sustituimos las indeterminadas $X_i$ por $k$ conjuntos de valores concretos, lo que nos establece un sistema lineal de $k$ ecuaciones en los coeficientes, sistema que resolvemos por los métodos de álgebra lineal.

*Ejemplo* 4.6.10. Sea $f = (X_1 + X_2 - X_3 - X_4)(X_1 - X_2 + X_3 - X_4)(X_1 - X_2 - X_3 + X_4)$. Es fácil comprobar que $f$ es simétrico homogéneo de grado 3. La lista de todos los monomios posibles de peso 3 es la siguiente: $s_1^3, s_1s_2, s_3$. Así que expresamos

$$f = as_1^3 + bs_1s_2 + cs_3$$

Ahora consideramos tres conjuntos de valores para los $X_i$ de manera que nos quede un sistema determinado de tres ecuaciones lineales en $a, b, c$. Por ejemplo los valores

| $X_1$ | $X_2$ | $X_3$ | $X_4$ | $s_1$ | $s_2$ | $s_3$ |
|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 2 | 1 | 0 |
| 1 | 1 | 1 | 0 | 3 | 3 | 1 |

nos dan el sistema

$$\begin{aligned} f(1,0,0,0) &= 1 = a \\ f(1,1,0,0) &= 0 = 8a + 2b \\ f(1,1,1,0) &= -1 = 27a + 9b + c \end{aligned}$$

que tiene la solución $a = 1$, $b = -4$, $c = 8$. Luego

$$f = s_1^3 - 4s_1s_2 + 8s_3$$

Para ilustrar esta técnica propongo la siguiente actividad: Sea $n \geq 5$. Expresar el polinomio $f = \sum x_1^2x_2^2x_3$ como un polinomio en los simétricos elementales.

Otro tipo de polinomios interesantes son los definidos a continuación:

**Definición 4.6.11.** Un polinomio $f \in A[X_1, \ldots, X_n]$ se llama *alternado* si para toda permutación $\sigma \in s_n$ se verifica $\sigma \cdot f = sgn(\sigma)f$.

El polinomio alternado no nulo mas sencillo es el producto de todas las diferencias

$$\Delta = \prod_{i<j}(X_i - X_j)$$

Cada par ordenado de índices $i < j$ aparece exactamente una vez, así que en total hay $n(n-1)/2$ factores lineales y $\Delta$ es un polinomio homogéneo de grado $n(n-1)/2$. Cuando aplicamos una trasposición $(i\ j)$ a $\Delta$, los factores se permutan entre sí, excepto el factor $X_i - X_j$ que se transforma en $X_j - X_i$, luego $\Delta$ cambia de signo.

**Teorema 4.6.12.** *Sea $A$ un dominio de integridad de característica distinta de 2. Todo polinomio $f$ alternado de $A[X_1, \ldots, X_n]$ es de la forma $f = \Delta g$, donde $g$ es simétrico.*

*Demostración.* Sustituyendo $X_2 = X_1$ obtenemos

$$f(X_1, X_1, \ldots, X_n) = -f(X_1, X_1, \ldots, X_n)$$

y como $car(A) \neq 2$, necesariamente $f(X_1, X_1, \ldots, X_n) = 0$, luego $(X_1 - X_2)$ divide a $f$. De la misma forma $X_i - X_j$ divide a $f$ para todo par $i < j$. Como estos polinomios son primos relativos, su producto divide a $f$ así que existe un $g \in A[X_1, \ldots, X_n]$ con $f = \Delta g$. Claramente $g = f/\Delta$ es un polinomio simétrico. □

**Corolario 4.6.13.** *Sea $f \in A[X_1, \ldots, X_n]$ un polinomio alternado. Entonces $gr(f) \geq n(n-1)/2$.*

# 4.7. La resultante

## 4.7.1. Introducción

El problema fundamental de la teoría de eliminación es el siguiente: Dados dos polinomios con coeficientes en un cuerpo $F$:

$$\begin{array}{ll} f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0, & a_n \neq 0 \\ g = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0, & b_m \neq 0 \end{array} \tag{4.7.1}$$

determinar si tienen una raíz común en una extensión de $F$ y en caso afirmativo hallarla. Para responder a esta cuestión, se busca una expresión que se anule sólo cuando $f$ y $g$ tienen una raíz común y que además sea calculable como función racional de los coeficientes de $f$ y $g$. La más sencilla de tales expresiones es la resultante que vamos a definir y estudiar.

## 4.7.2. Definición

Sea $K$ un cuerpo de descomposición para $fg$, así que en $K[X]$ tenemos:

$$\begin{array}{l} f = a_n(X-\alpha_1)\ldots(X-\alpha_n) = a_n \prod_{i=1}^{n}(X-\alpha_i) \\ g = b_m(X-\beta_1)\ldots(X-\beta_m) = b_m \prod_{j=1}^{m}(X-\beta_j) \end{array} \tag{4.7.2}$$

La *resultante de f y g* viene definida por

$$R(f,g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) \tag{4.7.3}$$

## 4.7.3. Propiedades

1. $R(f,g) = 0 \Leftrightarrow \exists i, j$ tales que $\alpha_i = \beta_j$ (i.e., sii $f$ y $g$ tienen una raíz en común)
2. $R(g,f) = (-1)^{nm}R(f,g)$
3. $R(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(\beta_j)$
4. $R(fg,h) = R(f,h)R(g,h)$, $R(f,gh) = R(f,g)R(f,h)$
5. Si m = 0 (i.e. si $g = b$ es un escalar), $R(f,b) = b^n$
6. $R(X^k, f) = a_0^k$; $R(f, X^k) = (-1)^{nk}a_0^k$
7. Si $g = fq + r$, $R(f,g) = a_n^{gr(g)-gr(r)}R(f,r)$

   Demostración: $R(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = a_n^m \prod_{i=1}^{n}(f(\alpha_i)q(\alpha_i) + r(\alpha_i)) = a_n^n \prod_{i=1}^{n} r(\alpha_i) = a_n^{m-gr(r)}R(f,r)$
8. $R(X^k f, g) = b_0^k R(f,g)$; $R(f, X^k g) = (-1)^{nk}a_0^k R(f,g)$
9. $R(f,g)$ es un polinomio simétrico de grado m en las $\alpha_i$
10. $R(f,g)$ es un polinomio simétrico de grado n en las $\beta_j$
11. $R(f,g)$ es un polinomio homogéneo de grado m en las $a_i$

    Demostración: Por la propiedad 9, $R(f,g)$ es expresable como un polinomio en los polinomios simétricos elementales $\sigma_i = (-1)^i \frac{a_i}{a_0}$. Por el factor $a_0^m$ todos los denominadores se simplifican.

12. $R(f,g)$ es un polinomio homogéneo de grado n en las $b_j$

13. El término $a_n^m b_0^n$ tiene coeficiente +1 en $R(f,g)$
    Demostración: Dicho término sólo aparece al desarrollar $a_n^m b_m^n \prod_{i=1}^{n}(-\beta_n) = a_n^m b_0^n$.

## 4.8. El discriminante

El caso particular más importante de la resultante es cuando $g = f'$ (la derivada formal). En ese caso, $R(f,f') = 0 \Leftrightarrow f$ tiene raíces múltiples. Explícitamente, sean

$$f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 = a_n \prod_{i=1}^{n}(X - \alpha_i)$$

$$f' = n a_n X^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1 = a_n \sum_{j=1}^{n} \prod_{i\neq j}(X - \alpha_i)$$

$$f'(\alpha_j) = a_n \prod_{i\neq j}(\alpha_j - \alpha_i)$$

$$R(f,f') = a_n^{n-1} \prod_{j=1}^{n} f'(\alpha_j) = a_n^{2n-1} \prod_{j=1}^{n} \prod_{i\neq j}(\alpha_j - \alpha_i) \tag{4.8.1}$$

### 4.8.1. Definición

Llamamos *discriminante de* $f$ a $D(f) = a_n^{2n-2} \prod_{i<j}(\alpha_i - \alpha_j)^2$. Comparando con (4.8.1) obtenemos:

$$R(f,f') = (-1)^{\frac{n(n-1)}{2}} a_n D(f) \tag{4.8.2}$$

### 4.8.2. Propiedades

1. $f_1, f_2 \in F[X] \Rightarrow D(f_1 f_2) = D(f_1)D(f_2)R(f_1,f_2)^2$
2. $f_1, \ldots, f_r \in F[X] \Rightarrow D(f_1 \ldots f_r) = D(f_1)\ldots D(f_r)R^2$ con $R \in F$

## 4.9. Métodos de cálculo

En esta sección nos planteamos encontrar una expresión explícita (o un método de cálculo) para $R(f,g)$ y $D(f)$ en función de los coeficientes de $f$ y $g$. Para ello existen diversos métodos que pasamos a describir.

### 4.9.1. Cálculo directo

Las propiedades halladas para la resultante permiten calcular directamente el discriminante de polinomios particulares. Veamos algunos ejemplos:

1. Ejemplo: $f = X^n - 1 = \prod_{i=1}^{n}(X - \alpha_i)$, $f' = nX^{n-1}$

$$D(f) = (-1)^{\frac{n(n-1)}{2}} R(f, f') = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} n\alpha_i^{n-1} =$$

$$(-1)^{\frac{n(n-1)}{2}} n^n (\prod_{i=1}^{n}(\alpha_i))^{n-1} = (-1)^{\frac{n(n-1)}{2}+n(n-1)} n^n = (-1)^{\frac{n(n-1)}{2}} n^n$$

   En particular si $q$ es impar, $f = X^q - 1$, $D(f) = (-1)^{\frac{q-1}{2}} q^q$

2. Ejemplo: $f = X^{p-1} + X^{p-2} + \ldots + X + 1$ $\quad p$ primo impar. Sea $g = X - 1$. Entonces $fg = X^p - 1 \Rightarrow$ $D(fg) = (-1)^{\frac{p-1}{2}} p^p$
   $g' = 1 \Rightarrow D(g) = R(g, g') = 1 \qquad R(f, g) = f(1) = p.$
   Luego $D(fg) = D(f)D(g)R(f, g)^2 \Rightarrow D(f) = (-1)^{\frac{p-1}{2}} p^{p-2}$

3. Ejemplo:

$$f = X^3 + aX + b = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$
$$f' = 3X^2 + a \qquad D(f) = -R(f, f')$$
$$R(f, f') = \prod_{i=1}^{3}(3\alpha_i^2 + a) = \prod_{i=1}^{3} f'(\alpha_i)$$

   Pero $f'(\alpha_i) = 3\alpha_i^2 + a = \frac{3\alpha_i^3 + a\alpha_i}{\alpha_i} = \frac{-2a\alpha_i - 3b}{\alpha_i}$
   Llamamos $\beta_i = 2a\alpha_i + 3b \Rightarrow \alpha_i = \frac{\beta_i - 3b}{2a}$ así que $\beta_i$ es raíz de $(\frac{X-3b}{2a})^3 + a\frac{X-3b}{2a} + b \Rightarrow \beta_1\beta_2\beta_3 = 8a^3(\frac{27b^3}{8a^3} + \frac{3b}{2} - b)$ $= 27b^3 + 4a^3b$

$$R(f, f') = \prod_{i=1}^{3} f'(\alpha_i) = -\frac{\prod_{i=1}^{3}(2a\alpha_i + 3b)}{\prod_{i=1}^{3}\alpha_i} = -\frac{27b^3 + 4a^3b}{-b} = 27b^2 + 4a^3$$

   y por tanto $D(f) = -(4a^3 + 27b^2)$

4. Ejemplo:

$$f = X^3 + aX^2 + b = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$
$$f' = 3X^2 + 2aX = X(3X + 2a) \quad f'(\alpha_i) = \alpha_i(3\alpha_i + 2a)$$

   Sea $\beta_i = 3\alpha_i + 2a \Rightarrow \alpha_i = \frac{\beta_i - 2a}{3}$ y los $\beta_i$ son raíces de $(\frac{X-2a}{3})^3 + a(\frac{X-2a}{3})^2 + b \Rightarrow \beta_1\beta_2\beta_3 = 3^3((\frac{2a}{3})^3 - a(\frac{2a}{3})^2 - b)$ $= -(4a^3 + 27b)$
   Luego $R(f, f') = \prod_{i=1}^{3} f'(\alpha_i) = \prod_{i=1}^{3}\alpha_i \prod_{i=1}^{3}\beta_i = (-b)(-(4a^3 + 27b))$
   y $D(f) = -R(f, f') = -b(4a^3 + 27b)$

5. Ejemplo:

$$f = X^5 + aX + b = \prod_{i=1}^{5}(X - \alpha_i) \qquad f' = 5X^4 + a$$

$$f'(\alpha_i) = 5\alpha_i^4 + a = \frac{5\alpha_i^5 + a\alpha_i}{\alpha_i} = \frac{-4a\alpha_i - 5b}{\alpha_i}$$

Llamamos $\beta_i = 4a\alpha_i + 5b \Rightarrow \alpha_i = \frac{\beta_i - 5b}{4a}$ así que $\beta_i$ es raíz de $(\frac{X-5b}{4a})^5 + a\frac{X-5b}{4a} + b \Rightarrow \prod_{i=1}^5 \beta_i = (4a)^5((\frac{5b}{4a})^5 + \frac{5b}{4} - b) = (5b)^5 + 4^4a^5b$

$$D(f) = R(f, f') = \prod_{i=1}^{5} f'(\alpha_i) = -\frac{\prod_{i=1}^5 \beta_i}{\prod_{i=1}^5 \alpha_i} = 5^5b^4 + 4^4a^5$$

6. Ejemplo:

$$f = X^5 + aX^4 + b = \prod_{i=1}^{5}(X - \alpha_i)$$
$$f' = 5X^4 + 4aX^3 = X^3(5X + 4a) \quad f'(\alpha_i) = \alpha_i^3(5\alpha_i + 4a)$$

Sea $\beta_i = 5\alpha_i + 4a \Rightarrow \alpha_i = \frac{\beta_i - 4a}{5}$ y los $\beta_i$ son raíces de $(\frac{X-4a}{5})^5 + a(\frac{X-4a}{5})^4 + b \Rightarrow \prod_{i=1}^5 \beta_i = 5^5((\frac{4a}{5})^5 - a(\frac{4a}{5})^4 - b)$ $= -(4^4a^5 + 5^5b)$

Luego $D(f) = R(f, f') = \prod_{i=1}^5 f'(\alpha_i) = \prod_{i=1}^5 \alpha_i^3 \prod_{i=1}^5 \beta_i = b^3(4^4a^5 + 5^5b)$

7. Ejemplo:

$$f = X^n + aX + b = \prod_{i=1}^{n}(X - \alpha_i) \qquad f' = nX^{n-1} + a$$
$$f'(\alpha_i) = n\alpha_i^{n-1} + a = \frac{n\alpha_i^n + a\alpha_i}{\alpha_i} = \frac{-(n-1)a\alpha_i - nb}{\alpha_i}$$

Llamamos $\beta_i = (n-1)a\alpha_i + nb \Rightarrow \alpha_i = \frac{\beta_i - nb}{(n-1)a}$ así que $\beta_i$ es raíz de $(\frac{X-nb}{(n-1)a})^n + a\frac{X-nb}{(n-1)a} + b \Rightarrow \prod_{i=1}^n \beta_i = (-1)^n((n-1)a)^n(((-1)^n\frac{nb}{(n-1)a})^n - \frac{nb}{n-1} + b) = (nb)^n + (-1)^n(n-1)^{n-1}a^n(-b)$

$$R(f, f') = \prod_{i=1}^{n} f'(\alpha_i) = (-1)^n\frac{\prod_{i=1}^n \beta_i}{\prod_{i=1}^n \alpha_i} = n^nb^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n$$

$$D(f) = (-1)^{\frac{n(n-1)}{2}}R(f, f') = (-1)^{\frac{n(n-1)}{2}}(n^nb^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n)$$

8. Ejemplo:

$$f = X^n + aX^{n-1} + b = \prod_{i=1}^{n}(X - \alpha_i) \qquad f' = nX^{n-1} + (n-1)aX^{n-2} =$$
$$X^{n-2}(nX + (n-1)a) \qquad f'(\alpha_i) = \alpha_i^{n-2}(n\alpha_i + (n-1)a)$$

Sea $\beta_i = n\alpha_i + (n-1)a \Rightarrow \alpha_i = \frac{\beta_i - (n-1)a}{n}$ y los $\beta_i$ son raíces de $(\frac{X-(n-1)a}{n})^n + a(\frac{X-(n-1)a}{n})^{n-1} + b \Rightarrow \prod_{i=1}^n \beta_i$ $= (-1)^n(n^n((-\frac{(n-1)a}{n})^n + a(-\frac{(n-1)a}{n})^{n-1} - b)) = -(n-1)^{n-1}a^n + (-1)^nn^nb$

Luego $R(f, f') = \prod_{i=1}^n f'(\alpha_i) = \prod_{i=1}^n \alpha_i^{n-2} \prod_{i=1}^n \beta_i = (-b)^{n-2}(-(n-1)^{n-1}a^n + (-n)^nb)$

y $D(f) = (-1)^{\frac{n(n-1)}{2}}R(f, f') = (-1)^{\frac{(n-1)(n+2)}{2}}b^{n-2}((n-1)^{n-1}a^n + (-1)^{n-1}n^nb)$

### 4.9.2. Método modular

A partir de la propiedad 7 de la resultante puede desarrollarse un método muy económico para el cálculo de la resultante de algunos pares especiales de polinomios: En primer lugar, sean

$$f = a_n X^n + \ldots + a_0 \qquad g = X - b$$

Diviendo f entre g obtenemos:

$$f = gf_1 + f(b)$$

Por las propiedades de la resultante obtenemos:

$$R(f,g) = (-1)^n R(g,f) = (-1)^n R(g, f(b)) = (-1)^n f(b) \tag{4.9.1}$$

Sean ahora

$$f = a_n X^n + \ldots + a_0 \qquad g = b_m X^m + \ldots + b_0$$

y sean $p, q_i, r, s_j$ tales que

$$pg \prod_{i=1}^{k}(X - q_i) \equiv r \prod_{j=1}^{l}(X - s_j) \pmod{f} \tag{4.9.2}$$

Entonces

$$R(f,p)R(f,g)R(f, \prod_{i=1}^{k}(X - q_i)) = a_n^{m+k-l} R(f,r)R(f, \prod_{j=1}^{l}(X - s_j)) \tag{4.9.3}$$

Pero por (4.9.1)

$$R(f,p) = p^n \qquad R(f,r) = r^n$$

$$R(f, \prod_{i=1}^{k}(X - q_i)) = \prod_{i=1}^{k} R(f, X - q_i)) = \prod_{i=1}^{k}(-1)^n f(q_i)$$

$$R(f, \prod_{j=1}^{l}(X - s_i)) = \prod_{j=1}^{l} R(f, X - s_i)) = \prod_{j=1}^{l}(-1)^n f(s_i)$$

Despejando en (4.9.3),

$$R(f,g) = (-1)^{n(k+l)} a_n^{m+k-l} \frac{r^n}{p^n} \frac{\prod_{j=1}^{l} f(s_i)}{\prod_{i=1}^{k} f(q_i)}$$

Ejemplo: Sean

$$f = X^5 - X^2 + 15 \qquad g = f' = 5X^4 - 2X$$

Tomamos $k = 1$, $l = 2$, $p_1 = 1$, $p_0 = 0$ y calculamos:

$$Xg = 5X^5 - 2X^2 = 5f + 3X^2 - 75 \equiv 3(X-5)(X+5) \pmod{f}$$

$$D(f) = R(f,f') = (-1)^{5(1+2)} \frac{3^5 f(5) f(-5)}{f(0)} =$$

$$-3^5 \frac{(5^5 - 5^2 + 15)((-5)^5 - (-5)^2 + 15)}{15} = -3^5 \frac{10^2 - 5^{10}}{15} = 3^4 5(5^8 - 4)$$

### 4.9.3. Por el algoritmo de Euclides

Dividiendo $g$ por $f$ obtenemos $g = fq + r$ con $\mathrm{gr}(r) < \mathrm{gr}(f)$. Por las propiedades 7 y 2,

$$R(f,g) = a_n^{m-gr(r)} R(f,r) = (-1)^{mgr(r)} a_n^{m-gr(r)} R(r,f)$$

Por inducción sobre el grado llegamos a $\mathrm{gr}(r) = 0$ y aplicamos la propiedad 5.

1. Ejemplo:

$$\begin{gathered} f = aX + b \\ f' = a \\ R(f,f') = a \\ D(f) = 1 \end{gathered}$$

2. Ejemplo:

$$\begin{gathered} f = aX^2 + bX + c \\ f' = 2aX + b \\ f = (\tfrac{1}{2}X + \tfrac{b}{4a})f' + (c - \tfrac{b^2}{4a}) \\ R(f,f') = R(f',f) = (2a)^2 R(f', c - \tfrac{b^2}{4a}) = (2a)^2(c - \tfrac{b^2}{4a}) = a(4ac - b^2) \\ D(f) = (-1)^{\frac{2-1}{2}} \tfrac{1}{a} R(f,f') = b^2 - 4ac \end{gathered}$$

3. Ejemplo:

$$\begin{gathered} f = X^3 + aX + b \\ f' = 3X^2 + a \\ f = \tfrac{1}{2}Xf' + r \qquad r = \tfrac{2a}{3}X + b \\ f' = (\tfrac{9}{2a}X - \tfrac{27b}{4a^2})r + r_1 \qquad r_1 = \tfrac{27b^2+4a^3}{4a^2} \\ R(f,f') = R(f',f) = 3^2 R(f',r) = 3^2 R(r,f') = 3^2(\tfrac{2a}{3})^2 R(r,r_1) = 4a^2 \tfrac{27b^2+4a^3}{4a^2} \\ D(f) = -R(f,f') = -(4a^3 + 27b^2) \end{gathered}$$

### 4.9.4. Determinante de Euler-Sylvester-Cayley

Multiplicando $f$ sucesivamente por $1, X, \ldots, X^{m-1}$ y $g$ por $1, X, X^{n-1}$ e igualando a cero nos queda el siguiente sistema de $(n+m)$ ecuaciones en las $(n+m)$ incógnitas $1, X, X^2, \ldots, X^{n+m-1}$:

$$\begin{array}{rcccccccccccccc}
X^{m-1}f & = & a_nX^{n+m-1} & + & a_{n-1}X^{n+m-2} & + & \ldots & + & a_0X^{m-1} & & & & = & 0 \\
X^{m-2}f & = & & & a_nX^{n+m-2} & + & \ldots & + & a_1X^{m-1} & + & a_0X^{m-2} & & = & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
1f & = & & & & & & a_nX^n & + & \ldots & + & a_0 & = & 0 \\
X^{n-1}g & = & b_mX^{n+m-1} & + & b_{m-1}X^{n+m-2} & + & \ldots & + & b_0X^{n-1} & & & & = & 0 \\
X^{n-2}g & = & & & b_mX^{n+m-2} & + & \ldots & + & b_1X^{n-1} & + & b_0X^{n-2} & & = & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
1g & = & & & & & & b_mX^m & + & \ldots & + & b_0 & = & 0
\end{array}$$

Por el teorema de Rouché, este sistema tendrá solución si y sólo si el determinante de los coeficientes es cero. Este determinante se llama *resultante de Euler-Sylvester-Cayley*:

$$C(f,g) = \begin{vmatrix} a_n & a_{n-1} & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & b_m & b_{m-1} & \dots & b_0 \end{vmatrix}$$

Vamos a ver que $C(f,g) = R(f,g)$: Como $C(f,g) = C(a_n,\dots,a_0,b_m,\dots,b_0)$ y los $a_i$ y $b_j$ son polinomios simétricos en $\alpha_i$ y $\beta_j$ respectivamente, obtenemos que $C(f,g)$ es un polinomio simétrico en $\alpha_i$ y $\beta_j$. Por otra parte, si $f$ y $g$ tienen una raíz común, el anterior sistema lineal tiene solución, luego $\forall i,j\ (\alpha_i - \beta_j) \mid C(f,g) \Rightarrow R(f,g) \mid C(f,g)$. Contando grados vemos que el cociente tiene grado cero (i.e. es una constante). Luego $C(f,g) = \lambda R(f,g)$. Pero el término $a_n^m b_m^n$ aparece con coeficiente +1 en $C(f,g)$ y en $R(f,g) \Rightarrow \lambda = 1$.

1. Ejemplo: Tomando $f = aX^2 + bX + c, g = f' = 2aX + b$ tenemos:

$$R(f,g) = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = ab^2 + 4a^2c - 2ab^2 = a(4ac - b^2)$$

2. Ejemplo: $f = X^3 + aX + b, g = 3X^2 + a$

$$R(f,g) = \begin{vmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{vmatrix} = 4a^3 + 27b^2$$

### 4.9.5. Determinante de Bezout

La resultante de Cayley proporciona una expresión sencilla y elegante para $R(f,g)$. Sin embargo, el orden del determinante es $(m+n)$, muy alto para los cálculos prácticos. Vamos a desarrollar otro método basado en la misma idea pero donde el determinante que va a aparecer es de orden $\max(m,n)$. En primer lugar consideramos $m = n$, o sea que $f$ y $g$ son del mismo grado. Definimos los elementos:

$$c_{ij} = \begin{cases} a_j b_i - a_i b_j & \text{si } 0 \le i,j \le n \\ 0 & \text{en otro caso} \end{cases}$$

Obsérvese que $c_{ij} = -c_{ij}$ y que $c_{ii} = 0$.

Si todos los $c_{ij}$ son cero, existe un $\lambda$ tal que $g = \lambda f$. En lo que sigue excluimos este caso. Consideremos ahora los polinomios:

$$h_i = b_i f - a_i g \qquad i = 0,1,\dots,n \tag{4.9.4}$$

Si $c_{ij} \neq 0$, del sistema:

$$h_i = b_i f - a_i g$$
$$h_j = b_j f - a_j g$$

obtenemos:

$$f = \frac{a_j}{c_{ij}}h_i - \frac{a_i}{c_{ij}}h_j$$
$$g = \frac{b_j}{c_{ij}}h_i - \frac{b_i}{c_{ij}}h_j$$

luego $h_i, h_j$ tienen un cero en común si y sólo si $f$ y $g$ tienen un cero en común, y las raíces comunes de $f$ y $g$ son precisamente las raíces comunes a todos los $h_i$.

Formemos ahora los polinomios:

$$\begin{array}{lll} g_0 = h_n & = b_n f - a_n g & = \sum_i^{n-1} d_{0i}X^i \\ g_1 = xg_0 + h_{n-1} & = (b_n X + b_{n-1})f - (a_n X + a_{n-1})g & = \sum_i^{n-1} d_{1i}X^i \\ g_2 = xg_1 + h_{n-2} & = (b_n X^2 + b_{n-1}X + b_{n-2})f - (a_n X^2 + a_{n-1}X + a_{n-2})g & = \sum_i^{n-1} d_{2i}X^i \\ \vdots \quad \vdots & \vdots & \vdots \\ g_{n-1} = xg_{n-2} + h_1 & = (b_n X^{n-1} + \ldots + b_1)f - (a_n X^{n-1} + \ldots + a_1)g & = \sum_i^{n-1} d_{n-1i}X^i \end{array} \tag{4.9.5}$$

Los $g_i$ tienen un cero en común $\Leftrightarrow$ los $h_i$ tienen un cero en común $\Leftrightarrow$ $f$ y $g$ tienen un cero en común. Veamos la forma general de los coeficientes $d_{ki}$. Por construcción,
$d_{0i} = c_{ni}$, $\quad d_{ki} = d_{k-1,i-1} + c_{n-k,i}$. Demostraremos por inducción sobre k que

$$d_{ki} = \sum_{j=0}^{k} c_{n-j,i-k+j} \tag{4.9.6}$$

Para $k = 0$ es trivial. Supongamoslo cierto para $k-1$. Entonces

$$d_{ki} = d_{k-1,i-1} + c_{n-k,i} = \sum_{j=0}^{k-1} c_{n-j,i+j-k} + c_{n-k,i}$$

Las raíces comunes de $f$ y $g$ dan lugar a soluciones no triviales del sistema:

$$\begin{array}{r} d_{0n-1}X^{n-1} + \ldots + d_{01}X + d_{00}1 = 0 \\ d_{1n-1}X^{n-1} + \ldots + d_{11}X + d_{10}1 = 0 \\ \vdots \\ d_{n-1,n-1}X^{n-1} + \ldots + d_{n-1,1}X + d_{n-1,0}1 = 0 \end{array}$$

Llamamos *resultante de Bezout de f y g* al determinante de este sistema:

$$B(f,g) = \begin{vmatrix} d_{0n-1} & \ldots & d_{00} \\ \vdots & \vdots & \vdots \\ d_{n-1,n-1} & \ldots & d_{n-1,0} \end{vmatrix}$$

Como cada $c_{ij}$ es homogéneo de grado 1 en $a_i$ y en $b_j$, $d_{ki}$ también es homogéneo de grado 1 en ambos, y $B(f,g)$ es un polinomio homogéneo en las $a_i$ y en las $b_j$ de grado $2n$. Igual que para la resultante de Cayley, $B(f,g)$ es cero cuando $f$ y $g$ tienen una raíz en común, luego $B(f,g) = \lambda R(f,g)$ y contando grados, $\lambda \in F$.

Para determinar $\lambda$ observamos el término $a_n^n b_0^n$. En la resultante de Cayley este término sólo aparece en el desarrollo de la diagonal principal y por tanto tiene coeficiente +1. En $B(f,g)$ aparece en el producto

de todos los $c_{0n} = a_n b_0 - a_0 b_n$ de la diagonal secundaria, luego tiene coeficiente $sgn(\sigma)$ siendo $\sigma = (1\ n)(2\ n-1)\ldots$ luego $sgn(\sigma) = (-1)^{\frac{n(n-1)}{2}}$ y por tanto $\lambda = (-1)^{\frac{n(n-1)}{2}}$, $B(f,g) = (-1)^{\frac{n(n-1)}{2}} R(f,g)$.

En caso de que $gr(g) = m \leq gr(f) = n$, tomamos $g_1 = X^{n-m}g$, formamos la resultante de Bezout de $f$ y $g_1$ y utilizamos la propiedad 8 de $R(f,g)$:

$$B(f, X^{n-m}g) = (-1)^{\frac{n(n-1)}{2}} R(f, X^{n-m}g) = (-1)^{\frac{n(n-1)}{2}+n(n-m)} a_0^{n-m} R(f,g)$$

Para calcular el discriminante de un polinomio, $g = f'$, $m = n-1$ y nos queda:

$$B(f, Xf') = (-1)^{\frac{n(n-1)}{2}+n} a_0 R(f,f') = (-1)^n a_0 a_n D(f)$$

así que

$$D(f) = \frac{(-1)^n}{a_n a_0} B(f, Xf')$$

además, en este caso los $c_{ij}$ tienen una forma sencilla: Sean

$$\begin{aligned} f &= a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0 \\ g = Xf' &= n a_n X^n + \ldots + a_1 X = b_n X^n + \ldots + b_1 \end{aligned}$$

luego $b_i = i a_i$, $c_{ij} = (j-i) a_i a_j$, y

$$d_{ki} = \sum_{j=0}^{k} c_{n-j,i+j-k} = \sum_{j=0}^{k} (i+2j-k-n) a_{n-j} a_{i+j-k} = -\sum_{j=0}^{k} (n-i+k-2j) a_{n-j} a_{i+j-k}$$

y nos queda la expresión:

$$D(f) = \frac{1}{a_n a_0} \begin{vmatrix} -d_{0,n-1} & \ldots & -d_{0,0} \\ \vdots & \ddots & \vdots \\ -d_{n-1,n-1} & \ldots & -d_{n-1,0} \end{vmatrix}$$

1. Ejemplo: $f = aX^2 + bX + c$

$$D(f) = \frac{1}{ac} \begin{vmatrix} ab & 2ac \\ 2ac & bc \end{vmatrix} = b^2 - 4ac$$

2. Ejemplo: $f = X^3 + aX + b$

$$D(f) = \frac{1}{b} \begin{vmatrix} 0 & 2a & 3b \\ 2a & 3b & 0 \\ 3b & 0 & ab \end{vmatrix} = -(4a^3 + 27b^2)$$

3. Ejemplo: $f = a_3X^3 + a_2X^2 + a_1X + a_0$

$$D(f) = \frac{1}{a_3 a_0} \begin{vmatrix} a_3a_2 & 2a_3a_1 & 3a_3a_0 \\ 2a_3a_1 & 3a_3a_0 + a_2a_1 & 2a_2a_0 \\ 3a_3a_0 & 2a_2a_0 & a_1a_0 \end{vmatrix}$$

4. Ejemplo: $f = a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$

$$D(f) = \frac{1}{a_4 a_0} \begin{vmatrix} a_4a_3 & 2a_4a_2 & 3a_4a_1 & 4a_4a_0 \\ 2a_4a_2 & 3a_4a_2 + a_3a_2 & 4a_4a_0 + 2a_3a_1 & 3a_3a_0 \\ 3a_4a_1 & 4a_4a_0 + 2a_3a_1 & 3a_3a_0 + a_2a_1 & 2a_2a_0 \\ 4a_4a_0 & 3a_3a_0 & 2a_2a_0 & a_1a_0 \end{vmatrix}$$

5. Ejemplo: $f = a_5X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$

$$D(f) = \frac{1}{a_5a_0}\begin{vmatrix} a_5a_4 & 2a_5a_3 & 3a_5a_2 & 4a_5a_1 & 5a_5a_0 \\ 2a_5a_3 & 3a_5a_2 + a_4a_3 & 4a_5a_1 + 2a_4a_2 & 5a_5a_0 + 3a_4a_1 & 4a_4a_0 \\ 3a_5a_2 & 4a_5a_1 + 2a_4a_2 & 5a_5a_0 + 3a_4a_2 + a_3a_2 & 4a_4a_0 + 2a_3a_1 & 3a_3a_0 \\ 4a_5a_1 & 5a_5a_0 + 3a_4a_1 & 4a_4a_0 + 2a_3a_1 & 3a_3a_0 + a_2a_1 & 2a_2a_0 \\ 5a_5a_0 & 4a_4a_0 & 3a_3a_0 & 2a_2a_0 & a_1a_0 \end{vmatrix}$$

## 4.10. Ejercicios

**Ejercicio 4.1.** Encontrar un polinomio $f(x) \in \mathbb{Q}[x]$ de grado 3 tal que: $f(0) = 6$, $f(1) = 12$ y $f(x) \equiv (3x + 3)$ *mod* $(x^2 + x + 1)$.

**Ejercicio 4.2.** Demostrar que el DFU $\mathbb{Z}[x]$ no es un DIP viendo que el ideal suyo generado por 2 y $x$ no es principal.

**Ejercicio 4.3.** Encontrar los polinomios irreducibles de grados 2 y 3 en $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ y $\mathbb{Z}_5[x]$.

**Ejercicio 4.4.** Estudiar si los siguientes polinomios son reducibles ó irreducibles en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$:

a) $2x^5 - 6x^3 + 9x^2 - 15$

b) $x^4 + 15x^3 + 7$

c) $x^5 + x^4 + x^2 + x + 2$

ch) $2x^4 + 3x^3 + 3x^2 + 3x + 1$

d) $x^4 - 22x^2 + 1$

e) $x^3 + 17x + 36$

f) $x^5 - x^2 + 1$

g) $x^4 + 10x^3 + 5x^2 - 2x - 3$

h) $x^4 + 6x^3 + 4x^2 - 15x + 1$

i) $x^4 - x^2 - 2x - 1$

j) $x^5 + 5x^4 + 7x^3 + x^2 - 3x - 11$

k) $x^5 - 10x^4 + 36x^3 - 53x^2 + 26x + 1$

l) $x^4 + 6x^3 + 4x^2 - 15x + 1$

ll) $x^4 + 3x^3 + 5x^2 + 1$

m) $x^6 + 3x^5 - x^4 + 3x^3 + 3x^2 + 3x - 1$

n) $x^4 + 4x^3 - x^2 + 4x + 1$

ñ) $x^5 - 6x^4 + 3x^3 + 2x - 1$

o) $2x^4 + 2x^3 + 6x^2 + 4$

p) $3x^5 - x^4 - 4x^3 - 2x^2 + 2x + 1$

q) $x^4 - x^3 + 9x^2 - 4x - 1$

r) $x^7 + 5x^6 + x^2 + 6x + 5$

s) $3x^5 + 42x^3 - 147x^2 + 21$

t) $x^5 + 3x^4 + 10x^2 - 2$

u) $x^4 + 3x^2 - 2x + 5$

v) $3x^6 + x^5 + 3x^2 + 4x + 1$

w) $2x^4 + x^3 + 5x + 3$

x) $2x^5 - 2x^2 - 4x - 2$

y) $3x^4 + 3x^3 + 9x^2 + 6$

z) $x^6 - 2x^5 - x^4 - 2x^3 - 2x^2 - 2x - 1$

$\alpha$) $6x^4 + 9x^3 - 3x^2 + 1$

$\beta$) $2x^4 + 8x^3 + 10x^2 + 2$

$\gamma$) $x^4 + 4x^3 + 6x^2 + 2x + 1$

$\delta$) $x^6 - x^5 + 3x^4 + x + 2$ sabiendo que reducido módulo 7, es producto de un polinomio de grado 1 por un irreducible de grado 5.

**Ejercicio 4.5.** Dado un anillo conmutativo y un elemento $a \in R$ demuestra que la aplicación $\Phi : R[x] \to R[x]$ dada por $\Phi(f(x)) = f(x + a)$ es un isomorfismo de anillos. Aplica este resultado y el criterio de Eisenstein para ver que el polinomio $f(x) = x^4 + 1$ es irreducible en $\mathbb{Z}[x]$ estudiando el polinomio $f(x+1)$.

**Ejercicio 4.6.** Estudiar si los siguientes polinomios son reducibles ó irreducibles en $\mathbb{Z}[x, y]$ y en $\mathbb{Q}[x, y]$:

a) $y^3 + x^2y^2 + xy + x$

b) $(y^5 - y^4 - 2y^3 + y - 1) + x(y - 2y^3) + x^2(y^4 + y^3 + 1) + x^3y^3$

c) $(x^4 + x + 1) + (1 - 2x - x^3)y + (x^3 + x)y^2$

d) $yx^3 + (-y^2 + y - 1)x^2 + (-y^2 + y - 1)x + (y^3 - y^2 - 1)$

e) $x^3y^2 + (x^2 + 1)y - x^2 - 1$

f) $y^2x + yx - y^2 + x - y - 1$

g) $2x^2y^3 + x^2y + x^2 + xy^4 + y^4 + 2y^3 + y + 1$

h) $2x^2y^2 + xy^3 + y^2 + x^2 + 1 + x^4y^2 - y - x^2y$

i) $x^3 + yx^2 + y^2x + y + 2x^2 - 4x$

**Ejercicio 4.7.** Sea $I$ el ideal de $\mathbb{Z}_3[x]$ generado por $x^2 + 2x + 2$. Demostrar que el anillo cociente $\mathbb{Z}_3[x]/I$ es un cuerpo y hallar el inverso de $(ax + b) + I$.

**Ejercicio 4.8.** Hallar el m.c.d. y el m.c.m. en $\mathbb{Z}_5[x]$ de los polinomios $x^7 + 2x^6 + 3x^5 + 3x^4 + 3x^3 + 3x^2 + 2x + 1$ y $3x^6 + 4x^4 + 4x^3 + 4x^2 + 3x + 1$.

**Ejercicio 4.9.** Calcular, si es posible, el inverso de la clase de $x$ en el anillo cociente $\mathbb{Q}[x]/(x^4 + x + 1)$.
Calcular también el inverso de la clase del polinomio $2x+1$ en el anillo cociente $\mathbb{Q}[x]/(x^3+2x^2+4x-2)$

**Ejercicio 4.10.** Demostrar que $\frac{\mathbb{Z}_2[x]}{(x^4+x+1)}$ es un cuerpo y calcular el inverso de la clase de $x^2 + 1$.

**Ejercicio 4.11.** Considerar el polinomio $f(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x]$:

- Probar que $f(x)$ es irreducible.

- Calcular el inverso de la clase $[x^2 + x + 2]$ en el anillo cociente $\mathbb{Z}_3[x]/f(x)\mathbb{Z}_3[x]$.
- ¿Es el polinomio $x^3 + 9x^2 - x + 244$ irreducible sobre $\mathbb{Z}[x]$?.

**Ejercicio 4.12.** Probar que el anillo cociente $\frac{\mathbb{Q}[x]}{(x^3-2x-3)}$ es un cuerpo y calcular el inverso de la clase de $x+1$.

**Ejercicio 4.13.** Calcular las unidades de los anillos cociente $\mathbb{Z}_5[x]/(x^2+x+1)$, $\mathbb{Z}_5[x]/(x^2+1)$ y $\mathbb{Z}_3[x]/(x^2+2)$.

**Ejercicio 4.14.** Hallar la intersección, la suma y el producto de los ideales de $\mathbb{Q}[x]$ generados por los polinomios $x^2 + x - 2$ y $x^2 - 1$.

**Ejercicio 4.15.** Demostrar que el subconjunto de $\mathbb{Z}[x]$ formado por los polinomios con coeficientes de grado uno par es un subanillo. Comprobar que en este subanillo los elementos 2 y $2x$ tienen m.c.d. y no tienen m.c.m.

**Ejercicio 4.16.** Estudiar si son cuerpos los siguientes anillos cociente $K[x]/I$:

a) $K = \mathbb{Q}$ ; $I = (x^2 + 2)$

b) $K = \mathbb{R}$ ; $I = (x^2 + 2)$

c) $K = \mathbb{Q}$ ; $I = (x^4 + 2x^3 + x^2 + 8x - 12)$

d) $K = \mathbb{Z}_3$ ; $I = (x^2 + x + 1)$

**Ejercicio 4.17.** Factorizar los siguientes polinomios como producto de irreducibles en $\mathbb{Z}[x]$:

1. $x^6 - x^5 - 10x^2 + 15x - 5$.
2. $3x^4 - 5x^3 - 101$.
3. $2x^4 + 4x - 1$.

**Ejercicio 4.18.** Factorizar en irreducibles de $\mathbb{Q}[x]$ los siguientes polinomios:

1. $2x^4 + 3x^3 + 3x^2 + 3x + 1$.
2. $x^4 + 3x^3 + 5x^2 + 1$.
3. $x^5 - 4x + 1$.

**Ejercicio 4.19.** Para tres variables, expresar los siguientes polinomios simétricos como polinomios en los polinomios simétricos elementales:
$\sum x_i^2$ ; $\sum x_i^3$ ; $\sum x_i^4$ ; $\sum x_i^5$ .

**Ejercicio 4.20.** Expresar como polinomios en los polinomios simétricos elementales los polinomios siguientes que sean simétricos:

a) $(x + y)(y + z)(z + x)$

b) $(x + y - z)(y + z - x)(z + x - y)$

c) $(x^2 + x + 1)(y^2 + y + 2)(z^2 + z + 3)$

d) $(x^2 + y^2)(y^2 + z^2)(z^2 + x^2)$

e) $(x + y + z)^3 + (x + y + t)^3 + (x + z + t)^3 + (y + z + t)^3$

f) $x^2y + y^2x + x^2z + z^2x + y^2z + z^2y + xyz$

**Ejercicio 4.21.** Determinar el polinomio simétrico en tres variables de menor grado que es múltiplo de $x - 2y$. Expresarlo como polinomio en los polinomios simétricos elementales.

**Ejercicio 4.22.** Si $\alpha_1, \alpha_2, \alpha_3$ son las raices del polinomio $x^3 - 2x^2 + 3x - 1$, calcular el valor de la siguiente expresión:$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 - \alpha_1^2(\alpha_2 + \alpha_3) - \alpha_2^2(\alpha_1 + \alpha_3) - \alpha_3^2(\alpha_1 + \alpha_2) - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)$.

**Ejercicio 4.23.** Sea $f(x) = x^3 - 7x^2 - 8x + 9 \in \mathbb{Q}[x]$. Si $\alpha_1, \alpha_2, \alpha_3$ son las raices de $f(x)$, determinar el valor de $\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2$.

**Ejercicio 4.24.** Estudiar si los polinomios de $\mathbb{Q}[x]$, $x^4 + x^3 + 3x^2 + x + 2$ y $x^5 + x^3 - x^2 + 2x - 1$ tiene algun factor común no constante.

**Ejercicio 4.25.** Demostrar que el discriminante de la cúbica $ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ es $b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$.

**Ejercicio 4.26.** Hallar el discriminante de las siguientes cuárticas:

a) $x^4 + ax^3 + bx + c$

b) $x^4 + ax^2 + bx + c$

c) $x^4 + ax^3 + bx^2 + c$

**Ejercicio 4.27.** Se considera el polinomio $f(x) = x^3 - 4x^2 + 5x + k \in \mathbb{Z}[x]$. Hallar $k$ para que $f(x)$ tenga una raiz doble y calcular para ese valor de $k$ las raices del polinomio $f(x)$.

**Ejercicio 4.28.** Demostrar que $f(x) = x^3 + 2x^2 + 5x + k \in \mathbb{Z}[x]$ es irreducible si $k$ es impar. Demostrar que $f(x)$ no tiene raices múltiples cualquiera que sea el valor de $k$. Si $k$ es impar ¿Son cuerpos los anillos cociente $\mathbb{Q}[x]/(f(x))$ y $\mathbb{R}[x]/(f(x))$?.

**Ejercicio 4.29.** Encuentra tres números cuya suma es 2, la suma de sus cuadrados es 2 y la de sus cubos es 8.

**Ejercicio 4.30.** Sean $\alpha_1$, $\alpha_2$ y $\alpha_3$ las raíces del polinomio $x^3 + 2x^2 - x + 3$. Halla el polinomio cuyas raíces son $(\alpha_1\alpha_2)^{-1}$, $(\alpha_1\alpha_3)^{-1}$ y $(\alpha_2\alpha_3)^{-1}$.

**Ejercicio 4.31.** Halla el valor de k para que el polinomio $x^3 - 3x + k$ tenga una raíz doble.

**Ejercicio 4.32.** Halla el valor de k para que las raíces $\alpha_1$, $\alpha_2$ y $\alpha_3$ del polinomio $x^3 + 2x^2 - 7x + k$ verifiquen la relación $\alpha_1^2 = \alpha_2^2 + \alpha_3^2$.

**Ejercicio 4.33.** ¿Existe un valor entero para $k$ de forma que $x^2 - kx + 1$ y $x^3 + x^2 + 1$ tengan raíces comunes?

**Ejercicio 4.34.** Supongamos que $x_1, x_2$ y $x_3$ son las raíces de $x^3 + 2x - 2$. Calcular $x_1^2 + x_2^2 + x_3^2 - \frac{1}{2}(x_1^3 + x_2^3 + x_3^3)$.

**Ejercicio 4.35.**

1. Sea $f(x) = x^3 - x^2 - x + 19 \in \mathbb{Q}[x]$. Si $\alpha_1$, $\alpha_2$ y $\alpha_3$ son las raíces de $f(x)$, determinar el valor de $(\alpha_1 - \alpha_2)^2 + (\alpha_1 - \alpha_3)^2 + (\alpha_2 - \alpha_3)^2$.
2. Demostrar que $f(x) = x^3 + 2x^2 - 3x + k \in \mathbb{Z}[x]$ es irreducible si $k$ es impar. Demostrar que $f(x)$ no tiene raíces múltiples para ningún valor entero de $k$.

## 4.11. Polinomios usando GAP

### 4.11.1. Coeficientes

Como ya hemos visto con anterioridad, para empezar a trabajar con polinomios, tenemos que especificar las variables y qué anillo de coeficientes vamos a considerar. GAPpor defecto expande las expresiones que introducimos, a diferencia de MATHEMATICA.

```
gap> x:=Indeterminate(Rationals,"x");
x
gap> (x+1)*(x-1);
x^2-1
```

Si queremos obtener una lista de los coeficientes de un polinomio en una variable, podemos usar lo siguiente.

```
gap> CoefficientsOfUnivariatePolynomial(x^2+x-1);
[ -1, 1, 1 ]
```

Y el polinomio líder lo obtenemos con `LeadingCoefficient`.

```
gap> LeadingCoefficient(x^2+x-1);
1
```

Definamos una función para encontrar el término líder de un polinomio respecto de una variable. En ella usamos funciones que son alternativa a las que acabamos de ver para más de una variable.

```
terminolider:=function(p,x)
    local grado;
    grado:=DegreeIndeterminate(p,x);
    return PolynomialCoefficientsOfPolynomial(p,x)[grado+1]*x^grado;
end;

gap> terminolider(x^2+x-1,x);
x^2
gap> terminolider(3*x^2+x-1,x);
3*x^2
gap> y:=Indeterminate(Rationals,"y");
y
gap> terminolider(y*x^2+y^4*x-1,x);
x^2*y
```

### 4.11.2. División

Si el anillo de coeficientes que consideramos es un cuerpo, entonces sabemos que el anillo de polinomios sobre una sola variable es un dominio euclídeo. Por tanto, podemos usar las funciones que ya conocemos para calcular el cociente y resto de una división.

```
gap> x:=Indeterminate(Rationals,"x");
x
gap> QuotientRemainder(x^3-x+1,2*x^2-3);
[ 1/2*x, 1/2*x+1 ]
```

Si nuestro anillo de polinomios no es un dominio euclídeo, entonces no podemos usar estas funciones.

```
gap> y:=Indeterminate(Rationals,"y");
y

gap> QuotientRemainder((x^3-x+1)*(y-1),y-1);
Error, no method found! For debugging hints type ?Recovery from NoMethodFound
Error, no 2nd choice method found for ‘QuotientRemainder’ on 3 arguments calle\
d from
QuotientRemainder( DefaultRing( [ r, m ] ), r, m ) called from
<function>( <arguments> ) called from read-eval-loop
Entering break read-eval-print loop ...
you can 'quit;' to quit to outer loop, or
you can 'return;' to continue
brk>
```

Ahora bien, si que podemos usar la función `Quotient` que nos da el cociente, en caso de que éste pertenezca a nuestro anillo de polinomio, y `fail` en caso contrario.

```
gap> Quotient((x^3-x+1)*(y-1),y-1);
x^3-x+1

gap> Quotient(2,3);
fail
```

(Esta última instrucción viene a decir que el cociente de dos entre tres no es entero, pues considera los argumentos de la función como enteros.)

### 4.11.3. Factorización

Si lo que queremos es factorizar polinomios, primero tenemos que definir la variable, e indicar cuál es el anillo de coeficientes para nuestros polinomios. Luego se usa `Factors` igual que antes.

```
gap> x:=Indeterminate(ZmodnZ(5),"x");
x
gap> Factors(x^2+1);
[ x+Z(5), x+Z(5)^3 ]
gap> Int(Z(5));
2
gap> Int(Z(5)^3);
3
```

Si cambiamos el anillo base, el resultado puede verse alterado.

```
gap> x:=Indeterminate(Rationals,"x");
x
gap> Factors(x^2+1);
[ x^2+1 ]

gap> x:=Indeterminate(Rationals,"x");
x
```

```
gap> Factors(x^3-1);
[ x-1, x^2+x+1 ]
gap> x:=Indeterminate(ZmodnZ(3),"x");
x
gap> Factors(x^3-1);
[ x-Z(3)^0, x-Z(3)^0, x-Z(3)^0 ]
```

Lo mismo ocurre con las raices y con el hecho de ser irreducible.

```
gap> x:=Indeterminate(ZmodnZ(3),"x");
x
gap> RootsOfUPol(x^3-1);
[ Z(3)^0, Z(3)^0, Z(3)^0 ]
gap> x:=Indeterminate(Rationals,"x");
x
gap> RootsOfUPol(x^3-1);
[ 1 ]

gap> x:=Indeterminate(ZmodnZ(3),"x");
x
gap> IsIrreducible(x^2+1);
true

gap> x:=Indeterminate(ZmodnZ(2),"x");
x
gap> IsIrreducible(x^2+1);
false
```

Veamos ahora a modo de ejemplo cómo calcular todos los polinomios irreducibles hasta un determinado grado en $\mathbb{Z}_m$. Empezamos definiendo una función que nos genere todos los polinomios hasta un determinado grado.

```
polshastagradomodm:=function(n,x,m)
    local ps;
    if (n=0) then
        return [0..(m-1)];
    fi;

    ps:=polshastagradomodm(n-1,x,m);
    return List(Cartesian(ps,List([0..(m-1)],i->i*x^n)),Sum);
end;
```

Así todos los polinomios en $\mathbb{Z}_3$ de grado menor o igual que dos son:

```
gap> polshastagradomodm(2,x,3);
[ 0*Z(3), x^2, -x^2, x, x^2+x, -x^2+x, -x, x^2-x, -x^2-x, Z(3)^0, x^2+Z(3)^0,
  -x^2+Z(3)^0, x+Z(3)^0, x^2+x+Z(3)^0, -x^2+x+Z(3)^0, -x+Z(3)^0,
  x^2-x+Z(3)^0, -x^2-x+Z(3)^0, -Z(3)^0, x^2-Z(3)^0, -x^2-Z(3)^0, x-Z(3)^0,
  x^2+x-Z(3)^0, -x^2+x-Z(3)^0, -x-Z(3)^0, x^2-x-Z(3)^0, -x^2-x-Z(3)^0 ]
```

De entre ellos podemos escoger los que son irreducibles.

```
gap> Filtered(last,IsIrreducible);
[ x, -x, x^2+Z(3)^0, x+Z(3)^0, -x^2+x+Z(3)^0, -x+Z(3)^0, -x^2-x+Z(3)^0,
  -x^2-Z(3)^0, x-Z(3)^0, x^2+x-Z(3)^0, -x-Z(3)^0, x^2-x-Z(3)^0 ]
```

Y si queremos quedarnos con un representante salvo asociados, podemos usar lo siguiente.

```
gap> Set(last,StandardAssociate);
[ x, x+Z(3)^0, x-Z(3)^0, x^2+Z(3)^0, x^2+x-Z(3)^0, x^2-x-Z(3)^0 ]
```

Para finalizar esta sección, implementamos una función que da los primos que se pueden aplicar en el criterio de Eisenstein para un polinomio en una variable.

```
eisenstein:=function(p)
    local lc,fp;
    lc:=CoefficientsOfUnivariatePolynomial(p);
    lc:=lc{[1..(Length(lc)-1)]};
    fp:=Factors(lc[1]);
    return Filtered(fp,f->(ForAll(lc,c->(c mod f=0)) and (lc[1] mod f^2=0)));
end;

gap> x:=Indeterminate(Rationals,"x");
x
gap> eisenstein(x^2+2*x-6);
[  ]
gap> eisenstein(x^2+2*x-4);
[ -2, 2 ]
```

### 4.11.4. Polinomios simétricos

Seguimos en esta sección la demostración dada en teoría para encontrar la expresión de un polinomio simétrico en función de los polinomios simétricos elementales.

Empezamos construyendo de forma recursiva el conjunto de polinomios simétricos elementales en un número determinado de variables (el argumento `x` contiene la lista de variables).

```
simetricoselementales:=function(x)
    local el;
    if (Length(x)=1) then
        return x;
    fi;
    el:=Concatenation([1],simetricoselementales(x{[2..Length(x)]}),[0]);
    return List([2..Length(el)],i->x[1]*el[i-1]+el[i]);
end;

gap> x:=Indeterminate(Rationals,"x");
x
gap> y:=Indeterminate(Rationals,"y");
y
gap> z:=Indeterminate(Rationals,"z");
z

gap> simetricoselementales([x,y,z]);
[ x+y+z, x*y+x*z+y*z, x*y*z ]
```

Vamos a identificar los polinomios simétricos elementales con las variables de entrada. Así si tenemos dos variables $x$ e $y$, éstas vistas como polinomios simétricos elementales denotan también respectivamente a $x + y$ y $xy$. Para traducir esta representación a notación estándar, usamos la siguiente función.

```
evaluasim:=function(f,x)
    if (IsRat(f)) then
        return f;
    fi;
    return Value(f,x,simetricoselementales(x));
end;
```

(La función `Value` sirve para evaluar un polinomio en varias variables. Si la entrada es un racional, no sabe hacer dicha evaluación. Es por eso que hemos puesto ese condicional al principio de la función.)

Ya tenemos pues los ingredientes necesarios para implementar el algoritmo.

```
sim:=function(f,x)
    local f0,f1,f2,g1,g2;

    if (Length(x)=1) or (IsRat(f)) then
        return f;
    fi;

    f0:=Value(f,[x[Length(x)]],[0]);
    if f0=0 then
        return 0;
    fi;
    g1:=sim(f0,x{[1..(Length(x)-1)]});
    f1:=f-evaluasim(g1,x);
    if f1=0 then
        return g1;
    fi;
    f2:=Quotient(f1,Product(x));
    g2:=sim(f2,x);
    return g1+x[Length(x)]*g2;

end;

gap> sim((x+y)*(y+z)*(z+x),[x,y,z]);
x*y-z
gap> evaluasim(last,[x,y,z]);
x^2*y+x^2*z+x*y^2+2*x*y*z+x*z^2+y^2*z+y*z^2
gap> (x+y)*(y+z)*(z+x);
x^2*y+x^2*z+x*y^2+2*x*y*z+x*z^2+y^2*z+y*z^2
```

### 4.11.5. Resultante y discriminante

Para calcular la resultante y el discriminante podemos usar las funciones `Resultant` y `Discriminant`, respectivamente.

```
gap> x:=Indeterminate(Rationals,"x");
```

```
x
gap> y:=Indeterminate(Rationals,"y");
y
gap> Resultant(x^2+y^2-1,x-y,y);
2*x^2-1

gap> Discriminant(x^3+1);
-27
gap> z:=Indeterminate(Rationals,"z");
z
gap> Discriminant(x^3+y*x^2+z,x);
-4*z*y^3-27*z^2
```

### 4.11.6. Cociente por un ideal

Intentemos calcular los divisores de cero y unidades del anillo cociente $R = \mathbb{Z}_2[x]/(x^2+1)$. Empezamos definiendo nuestra variable y el módulo.

```
gap> x:=Indeterminate(ZmodnZ(2),"x");
x

gap> modulo:=x^2+1;
x^2+Z(2)^0
```

Como cada elemento en $R$ tiene un único representante de grado menor o igual que uno (el resto de dividir por $x^2+1$), podemos identificar $R$ con el siguiente conjunto.

```
gap> elementos:=List(Cartesian([0..1],[0..1]),n->n[1]+x*n[2]);
[ 0*Z(2), x, Z(2)^0, x+Z(2)^0 ]
```

Que se lee como $\{0, x, 1, 1+x\}$. Seleccionamos aquellos elementos que son no nulos.

```
gap> elementosnonulos:=elementos{[2..4]};
[ x, Z(2)^0, x+Z(2)^0 ]
```

Así las unidades se pueden calcular de la siguiente forma.

```
gap> Filtered(elementosnonulos,n->
    ForAny(elementosnonulos,m->IsOne(EuclideanRemainder(n * m,modulo))));
[ x, Z(2)^0 ]
```

Obsérvese que hemos vuelto a utilizar `EuclideanRemainder`. La función `IsOne` sirve para determinar si un elemento en $\mathbb{Z}_2[x]$ es uno (no podemos en este caso escribir simplemente `EuclideanRemainder(n * m,modulo)=1`).

Los divisores de cero no nulos, se calculan de forma análoga.

```
gap> Filtered(elementosnonulos,
n->ForAny(elementosnonulos,
m->IsZero(EuclideanRemainder(n * m,modulo))))
[ x+Z(2)^0 ]
```

## 4.12. Aritmética en Anillos de Polinomios con MATHEMATICA

### 4.12.1. Generalidades

- **Producto de polinomios**

  El producto de dos polinomios $p$ y $q$ es $p\ q$ (o $p * q$). MATHEMATICAno devuelve el resultado a no ser que se lo pidamos con el comando `Expand`.

  Ejemplo:

```
In[1]:= p=2x^3+3x^2+7x+9;
In[2]:= q=6x^2+5x+4;
In[3]:= p q
```

```
Out[3]= (4 + 5x + 6x^2)(9 + 7x + 3x^2 + 2x^3)
```

```
In[4]:= Expand[p q]
```

```
Out[4]= 36 + 73x + 101x^2 + 65x^3 + 28x^4 + 12x^5
```

  Si queremos encontrar el resultado módulo $n$, entonces usamos el comando `PolynomialMod`.

  Ejemplo

```
In[5]:= PolynomialMod[p q,12]
```

```
Out[5]= x + 5x^2 + 5x^3 + 4x^4
```

  La opción `Modulus -> k` devuelve directamente el resultado módulo $k$.

  Ejemplo

```
In[6]:= Expand[p q,Modulus->12]
```

```
Out[6]= x + 5x^2 + 5x^3 + 4x^4
```

- **Coeficientes y coeficiente líder**

  La función `Exponent` nos dice el grado de un polinomio en la variable que queramos. Así, si

```
In[7]:= p=3x^3+5x+2;
q=x^4+2x+3x^2+5x+8;
```

  entonces

```
In[9]:= Exponent[p,x]
```

```
Out[9]= 3
```

mientras que

```
In[10]:= Exponent[q,x]
```

```
Out[10]= 4
```

El comando `Coefficient` puede ser usado para obtener el coeficiente que acompañe a una potencia de una variable.

Ejemplo

```
In[11]:= Coefficient[p,x,2]
```

```
Out[11]= 0
```

La lista de coeficientes la podemos obtener poniendo

```
In[12]:= CoefficientList[p,x]
```

```
Out[12]= {2, 5, 0, 3}
```

Usando el producto escalar, recuperamos el polinomio a partir de los coeficientes. Ejemplo

```
In[13]:= {2,5,0,3}.{1,x,x^2,x^3}
```

```
Out[13]= 2 + 5x + 3x^3
```

O bien

```
In[14]:= {2,5,0,3}.Table[x^i,{i,0,3}]
```

```
Out[14]= 2 + 5x + 3x^3
```

Definimos una función que nos da el coeficiente lider de un polinomio en una variable poniendo

```
In[15]:= coeficientelider[p_,x_]:=Last[CoefficientList[p,x]]
```

Así

```
In[16]:= coeficientelider[p,x]
```

```
Out[16]= 3
```

mientras que

```
In[17]:= coeficientelider[q,x]
```

```
Out[17]= 1
```

El comando `FullForm` nos da la representación interna de la expresión de un polinomio. Ejemplo

```
In[18]:= FullForm[p]
```

```
Out[18]//FullForm= Plus[2, Times[5, x], Times[3, Power[x, 3]]]
```

Entonces, usando la función `Collect`, podemos también definir una función que nos dé el término líder (como se ve en la implementación de la función, `Last` también se puede aplicar a expresiones que no son listas).

```
In[19]:= terminolider[p_,x_]:=Last[Collect[p,x]]
```

Así

```
In[20]:= terminolider[p,x]
```

```
Out[20]= 3x^3
```

mientras que

```
In[21]:= terminolider[p q,x]
```

```
Out[21]= 3x^7
```

- **Evaluación de un polinomio**
  Para evaluar un polinomio (o cualquier expresión) en un valor, usamos las reglas de sustitución

```
In[22]:= evalua[p_,x_,a_]:=p /. {x:>a}
```

Ejemplo

```
In[23]:= evalua[p,x,0]
```

```
Out[23]= 2
```

Para evaluar módulo *m,* hacemos lo siguiente.

```
In[24]:= evalua[p_,x_,a_,m_]:=Mod[evalua[p,x,a],m]
```

Ejemplo

```
In[25]:= evalua[q,x,0,3]
```

```
Out[25]= 2
```

Si nos interesa evaluar un polinomio en más de un elemento también podemos usar la función `evalua` aplicada a listas poniendo

```
In[26]:= SetAttributes[evalua,Listable]
```

Así

```
In[27]:= evalua[1+x^2,x,{1,2,3}]
```

```
Out[27]= {2, 5, 10}
```

mientras que si evaluamos y tomamos módulo

```
In[28]:= evalua[{1+x^3,1+x^2},x,1,2]
```

```
Out[28]= {0, 0}
```

y

```
In[29]:= evalua[{1+x^3,1+x^2},x,{0,1},3]
```

```
Out[29]= {1, 2}
```

y tomando varios módulos

```
In[30]:= evalua[1+x^2,x,1,{2,3,4,5}]
```

```
Out[30]= {0, 2, 2, 2}
```

Ejemplo: Si queremos obtener la gráfica del polinomio $p = x^3 + 3x^2 + 2x + 2$ visto como polinomio en $\mathbb{Z}_5$ declaramos el polinomio

```
In[31]:= p=x^3+3x^2+2x+2;
```

y ponemos

```
In[32]:= Map[{#,evalua[p,x,#,5]}&,Range[0,4]]
```

```
Out[32]= {0, 2, 1, 3, 2, 1, 3, 2, 4, 2}
```

- **Cociente y resto**

  Las funciones predefinidas que dan cociente y resto son `PolynomialQuotient` y `PolynomialRemainder`.

  Ejemplo

```
In[33]:= PolynomialQuotient[x^2-1,2x+2,x]
```

```
Out[33]= -(1/2) + x/2
```

  Ejemplo

```
In[34]:= PolynomialRemainder[x^2-1,2x+2,x]
```

```
Out[34]= 0
```

  Si para estas funciones queremos tomar módulo entonces usamos `PolynomialMod`

  Ejemplo

```
In[35]:= PolynomialMod[PolynomialRemainder[x^2+1,x+1,x],2]
```

```
Out[35]= 0
```

y

```
In[36]:= PolynomialMod[PolynomialQuotient[x^2+1,x+1,x],2]
```

```
Out[36]= 1 + x
```

### 4.12.2. Factorización

- **El contenido de un polinomio**

  Sabemos que se trata del máximo común divisor así que lo calculamos con la función

```
In[37]:= contenido[p_,x_]:=Apply[GCD,CoefficientList[p,x]]
```

  Ejemplo

```
In[38]:= contenido[105x^3-21x^2+70x-35,x]
```

```
Out[38]= 7
```

- **El comando `Factor`**

  Con este comando podemos calcular la factorización en $\mathbb{Z}[x]$ de un polinomio con coeficientes enteros. Si queremos que esa factorización se efectúe módulo $m$, entonces agregamos la opción `Modulus-> m`.

  Ejemplos

```
In[39]:= Factor[6x-4]
```

```
Out[39]= 2(-2 + 3x)
```

```
In[40]:= Factor[6x^3-19x^2-8x+12]
```

```
Out[40]= (-2 + 3x)(-6 - 5x + 2x^2)
```

```
In[41]:= Factor[x^4+x^3+x+2]
```

Out[41]= $2 + x + x^3 + x^4$

```
In[42]:= Factor[x^4+x^3+x+2,Modulus->3]
```

Out[42]= $(1 + x^2)(2 + x + x^2)$

- **La derivada de un polinomio**
  La función predefinida `D[f,x]` devuelve la derivada de $f$ respecto de $x$.
  Ejemplos

```
In[43]:= D[2x^5-7x^3+3x^2-5x+3,x]
```

Out[43]= $-5 + 6x - 21x^2 + 10x^4$

```
In[44]:= D[(3x+1)^100,x]
```

Out[44]= $300(1 + 3x)^{99}$

- **Encontrando las raices de un polinomio: El comando `Solve`**
  Declaramos el polinomio

```
In[45]:= p=6x^3-19x^2-8x+12;
```

y entonces, para calcular las raices, ponemos

```
In[46]:= Solve[p==0,x]
```

Out[46]= $\{\{x \to 2/3\}, \{x \to 1/4(5 - \sqrt{73})\}, \{x \to 1/4(5 + \sqrt{73})\}\}$

Si queremos las raices del polinomio reducido modulo 7 entonces ponemos

```
In[47]:= Solve[{p==0,Modulus==7},Mode->Modular]
```

```
Out[47]= {{Modulus-> 7, x → 3}}
```

de modo que la única raiz módulo 7 es 3.

Notemos que si factorizamos dicho polinomio $p$

```
In[48]:= Factor[p]
```

```
Out[48]= (-2 + 3x)(-6 - 5x + 2x^2)
```

mientras que si lo hacemos módulo 7

```
In[49]:= Factor[p,Modulus->7]
```

```
Out[49]= 6(4 + x)(4 + x + x^2)
```

de modo que, como habíamos visto arriba, la única raiz módulo 7 es $-4$, esto es, 3.

Ejercicio: Determina si los polinomios $x^3 + 2x + 2$ y $(x^4) + (x^3) + x + 2$ son reducibles módulo 3.

- **Polinomios de grado $n$ módulo $m$**

  Calculamos todos los polinomios de grado $n$ en $\mathbb{Z}_m[x]$. Para definir la correspondiente función recordemos que dadas dos listas, el comando `Outer` nos permite operar todos los miembros de la primera con los de la segunda mediante la operación que viene dada en el primer argumento. Luego, para que el resultado aparezca en una lista, usamos el comando `Flatten`.

  Entonces, si queremos calcular todos los polinomios de grado menor o igual que $n$ ponemos

```
In[50]:= polshastagrado[0,_,m_]:=Range[0,m-1];
polshastagrado[n_,x_,m_]:=With[{pn=polshastagrado[n-1,x,m]},
Union[pn,Flatten[Outer[Plus,Table[i x^n,{i,1,m-1}],pn]]]
]
```

  Ejemplo

```
In[52]:= polshastagrado[2,x,2]
```

```
Out[52]= {0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2}
```

  Mientras que si queremos calcular solo los de grado n ponemos

```
In[53]:= polsgrado[0,_,m_]:=Range[0,m-1];
polsgrado[n_,x_,m_]:=With[{pn=polshastagrado[n-1,x,m]},
Flatten[Outer[Plus,Table[i x^n,{i,1,m-1}],pn]]
]
```

Ejemplo

```
In[55]:= polsgrado[2,y,3]
```

```
Out[55]= {y^2, 1 + y^2, 2 + y^2, y + y^2, 2y + y^2, 1 + y + y^2, 2 + y + y^2, 1 + 2y + y^2, 2 + 2y + y^2, 2
y^2, 1 + 2y^2, 2 + 2y^2, y + 2y^2, 2y + 2y^2, 1 + y + 2y^2, 2 + y + 2y^2, 1 + 2y + 2
y^2, 2 + 2y + 2y^2}
```

A continuación queremos calcular los polinomios irreducibles módulo $m$ cuyo grado es menor o igual a $n$. Para ello tenemos en cuenta las siguientes observaciones:

1. `MemberQ` sirve para ver si un elemento pertenece a una lista.
2. `Function` sirve para definir una función que al primer argumento le asigna la regla que viene dada como segundo argumento.

Tenemos que calcular qué polinomios de grado $n$ no son divisibles por ningún polinomio irreducible de grado menor o igual a $n-1$. En la variable *pi* almacenaremos los polinomios irreducibles de grado menor o igual a $n-1$ (generados recursivamente), y en *ps* los polinomios mónicos de grado $n$.

Así, ponemos

```
In[56]:= polsirreduciblesgrado[1,x_,m_]:=Table[i+x,{i,0,m-1}]
```

y

```
In[57]:= polsirreduciblesgrado[n_,x_,m_]:=With[{pi=polsirreduciblesgrado[n-1,x,\
m],ps=x^n+polshastagrado[n-1,x,m]},
Union[pi,Select[ps,Not[MemberQ[Map[Function[z,PolynomialMod[\
PolynomialRemainder[#,z,x],m]],pi],0]]&]]
]
```

Ejemplo: Para calcular los irreducibles de grado 5 en $\mathbb{Z}_2[x]$ ponemos

```
In[58]:= polsirreduciblesgrado[5,x,2]
```

```
Out[58]= {x, 1 + x, 1 + x + x^2, 1 + x + x^3, 1 + x^2 + x^3, 1 + x + x^4, 1 + x^3 + x^4, 1 + x + x^2 + x^3 + x^4, 1 +
x^2 + x^5, 1 + x^3 + x^5, 1 + x + x^2 + x^3 + x^5, 1 + x + x^2 + x^4 + x^5, 1 + x + x^3 + x^4 + x^5,
1 + x^2 + x^3 + x^4 + x^5}
```

y para saber cuántos hay pedimos la longitud de la lista poniendo

```
In[59]:= Length[%]
```

```
Out[59]= 14
```

Y para calcular los irreducibles de grado 2 en $\mathbb{Z}_5[x]$ ponemos

```
In[60]:= polsirreduciblesgrado[2,x,5]
```

```
Out[60]= {x, 1 + x, 2 + x, 3 + x, 4 + x, 2 + x^2, 3 + x^2, 1 + x + x^2, 2 + x + x^2, 3 + 2x + x^2,
4 + 2x + x^2, 3 + 3x + x^2, 4 + 3x + x^2, 1 + 4x + x^2, 2 + 4x + x^2}
```

cuya longitud es

```
In[61]:= Length[%]
```

```
Out[61]=15
```

- **Raices racionales**

  Sabemos que las posibles raices racionales de un polinomio con coeficientes enteros son las fracciones que resultan de dividir los divisores del término independiente por los del coeficiente líder (notemos que MATHEMATICAautomáticamente simplifica fracciones). Definimos

```
In[62]:= posiblesraices[p_,x_]:=Module[{a0,an,salida},
a0=p/.x:>0;
an=coeficientelider[p,x];
salida=Flatten[Outer[Divide,Divisors[a0],Divisors[an]]];
Union[salida,-salida]
]
```

  Ejemplo: Si queremos calcular las posibles raices racionales del polinomio $6x^3 - 8$ ponemos

```
In[63]:= posiblesraices[6x^3-8,x]
```

```
Out[63]= {-8, -4, -8/3, -2, -4/3, -1, -2/3, -1/2, -1/3, -1/6, 1/6, 1/3, 1/2,
2/3, 1, 4/3, 2, 8/3, 4, 8}
```

  Análogamente

```
In[64]:= posiblesraices[6x^4+11x^3-19x^2+18x-8,x]
```

```
Out[64]= {-8, -4, -8/3, -2, -4/3, -1, -2/3, -1/2, -1/3, -1/6, 1/6, 1/3, 1/2,
2/3, 1, 4/3, 2, 8/3, 4, 8}
```

que en total son

```
In[65]:= Length[%]
```

```
Out[65]= 20
```

Ahora, para saber cuales de ellas son realmente raices del polinomio, evaluamos éste en toda la lista poniendo

```
In[66]:= evalua[6x^4+11x^3-19x^2+18x-8,x,%%]
```

```
Out[66]= {17576, 448, -2600/27, -112, -656/9, -50, -824/27, -91/4, -148/9,
-625/54, -197/36, -98/27, -2, 0, 8, 736/27, 136, 3752/9, 2000, 29128}
```

Observamos que sólo hay una raíz racional, a saber $\frac{2}{3}$

- **Un filtro**

```
In[67]:= posiblesraices[p_,x_,c_]:=Module[{pc,dpc},
pc=evalua[p,x,c];
dpc=Union[-Divisors[pc],Divisors[pc]];
Select[posiblesraices[p,x],MemberQ[dpc,Denominator[#]c-Numerator[#]]&]\
]
```

```
In[68]:= posiblesraices[6x^4+11x^3-19x^2+18x-8,x,1]
```

```
Out[68]= {-1, -1/3, 1/3, 1/2, 2/3, 4/3, 2}
```

```
In[69]:= posiblesraices[6x^4+11x^3-19x^2+18x-8,x,-1]
```

```
Out[69]= {-8/3, -2, -4/3, -2/3, -1/2, -1/3, -1/6, 2/3, 1, 4}
```

```
In[70]:= Intersection@@(posiblesraices[6x^4+11x^3-19x^2+18x-8,x,#]&/@{1,-1,2,-\
2})
```

```
Out[70]= {2/3}
```

O lo que es lo mismo (recuérdese que `Map` se usa para aplicar una función a cada uno de los elementos de una lista. `Apply` se puede usar para pasarle a una función como argumentos los elementos de una lista, aunque en realidad, lo que hace es cambiar la cabecera del segundo argumento por el primer argumento):

```
In[71]:= Apply[Intersection,Map[posiblesraices[6x^4+11x^3-19x^2+18x-8,x,#]&,{1,\
-1,2,-2}]]
```

```
Out[71]= 2/3
```

Ejercicio: Encuentra las posibles raices racionales de $72 - 24x - 18x^2 + 6x^3$.

- **Criterio de Eisenstein**

  Usamos el comando `FactorInteger` para implementar este criterio

```
In[72]:= eisenstein[p_,x_]:=With[{a0=p/.x:>0},Select[Map[First,FactorInteger[\
Abs[a0]]],(Union[Mod[Drop[CoefficientList[p,x],-1],#]]=={0}\[And]Mod[\
a0,#^2]!=0)&]!={}
]
```

Ejemplo

```
In[73]:= eisenstein[x^2+4x+4,x]
```

```
Out[73]= False
```

Ejercicio: ¿Se puede aplicar el criterio al polinomio $x^2 + 4x + 8$? ¿Y a $5x^5 + 6x^4 - 12x^2 + 18x - 24$?

### 4.12.3. Polinomios Simétricos

- **Los polinomios simétricos elementales**

  La siguiente función devuelve una lista con los polinomios simétricos elementales en las variables que introduzcamos

```
In[74]:= simetricoselementales[{x_}]:={x};
simetricoselementales[{x_,xs___}]:=With[{el=Join[{1},\
simetricoselementales[{xs}],{0}]},
Table[Expand[x el[[i-1]]+el[[i]]],{i,2,Length[el]}]
]
```

Ejemplo

```
In[76]:= simetricoselementales[{x,y,z,t}]
```

```
Out[76]= {t + x + y + z, tx + ty + xy + tz + xz + yz, txy + txz + tyz + xyz, txyz}
```

Ejercicio: Calcula los polinomios simétricos en cinco variables.

Introducimos a continuación la función `evalua` que sirve para evaluar un polinomio en varias variables. Nos será de utilidad para evaluar un polinomio en los polinomios simétricos elementales (compárese con la función `evalua` del principio de esta práctica). Usamos `ClearAll` para borrar su definición y hacer que MATHEMATICAse olvide de que tenía el atributo `Listable`.

```
In[77]:= ClearAll[evalua]
```

```
In[78]:= ?evalua
Global‘evalua
```

```
In[79]:= evalua[f_,{},{}]:=f;
evalua[f_,x_,v_]:=f/.Inner[Rule,x,v,List]
```

Ejemplo:

```
In[81]:= evalua[x y+z,{x,y},{1,2}]
```

```
Out[81]= 2 + z
```

La siguiente función nos sirve para expresar un polinomio que viene dado en función de los polinomios simétricos elementales en $n$ variables como un polinomio en esas variables. A los polinomios simétricos elementales en $n$ variables los vamos a denotar por $s_1, \ldots, s_n$.

```
In[82]:= Clear[s]
```

```
In[83]:= evaluasim[f_,x_]:=evalua[f,Table[Subscript[s, \
i],{i,1,Length[x]}],simetricoselementales[x]]
```

Así, el simétrico elemental de grado 1 en dos variables es

```
In[84]:= evaluasim[Subscript[s, 1],{x,y}]
```

Out[84]= $x + y$

mientras que el de grado dos es

```
In[85]:= evaluasim[Subscript[s, 2],{x,y}]
```

Out[85]= $x\,y$

Otros ejemplos son

```
In[86]:= evaluasim[Subscript[s, 1],{x,y,z}]
```

Out[86]= $x + y + z$

```
In[87]:= evaluasim[Subscript[s, 1]Subscript[s, 2]+Subscript[s, 3],{x,y,z}]
```

Out[87]= $xyz + (x + y + z)(xy + xz + yz)$

- **Expresando un polinomio simétrico en función de los polinomios simétricos elementales**

  Ya tenemos las piezas para implementar el algoritmo que expresa un polinomio simétrico en función de los polinomios simétricos elementales.

```
In[88]:= sim[f_]:=f /; Length[Variables[f]]==0
sim[f_]:=(f/.{Variables[f][[1]]:>Subscript[s, \
1]})/;Length[Variables[f]]==1
sim[f_]:=Module[{f0,f1,f2,g1,g2,var},
var=Variables[f];
f0=(f/.Last[var]->0);
g1=sim[f0];
(*Print["El polinomio que representa a ",f," con ",Last[var]," igual \
a cero es g1=",g1];*)
f1:=f-evaluasim[g1,var];
f2:=Simplify[f1/Times@@var];
(*Print["f1=",f1,", y así, f2=",f2];*)
g2:=sim[f2];
(*Print["El polinomio que representa a f2 es g2=",g2,", y obtenemos: \
",g1+Last[var] g2];*)
g1+Subscript[s, Length[var]] g2
]
```

Algunos ejemplos

```
In[91]:= sim[x y]
```

Out[91]= $s_2$

```
In[92]:= sim[x^2+y^2+z^2]
```

Out[92]= $s_1^2 - 2s_2$

```
In[93]:= sim[x y z]
```

Out[93]= $s_3$

```
In[94]:= sim[(x+y)^2+(x+z)^2+(y+z)^2]
```

Out[94]= $2s_1^2 - 2s_2$

```
In[95]:= sim[(x+y)(y+z)(z+x)]
```

Out[95]= $s_1 s_2 - s_3$

```
In[96]:= sim[(x+y-z)(y+z-x)(z+x-y)]
```

Out[96]= $s_1^3 + 4s_1 s_2 - 8s_3$

### 4.12.4. Resultante y discriminante

- **Resultante**

  La función `Resultant[polinomio, polinomio, variable]` calcula la resultante de dos polinomios

```
In[97]:= Resultant[x^3+5x+2,x^3-x-1,x]
```

```
Out[97]= -135
```

Ejercicio: Calcula los valores de $a$ para que los polinomios $f = a + 5x + ax + 6x^2 + x^3 + ax^3 + 5x^4 + x^5$ y $g = 2 + 7x + 8x^2 + 6x^3 + x^4$ tengan raíces comunes.

```
In[98]:= Solve[Resultant[x^5+5x^4+a x^3+6x^2+a x+a,x^4+6x^3+8x^2+7x+2,x]==0,a]
```

```
Out[98]= {{a → 1/2(7 - I √3)}, {a → 1/2(7 + I √3)},
{a → 2/47 (5 - 17 √17)}, {a → 2/47 (5 + 17 √17)}}
```

La resultante se puede usar para resolver sistemas de ecuaciones polinómicas en dos variables. Así, si queremos intersecar la circunferencia unidad con la bisectriz $x = y$, podemos usar el comando `Solve` de MATHEMATICA.

```
In[99]:= Solve[{x^2+y^2==1,x-y==0},{x,y}]
```

```
Out[99]= {{x → -1/√2, y → -1/√2}, {x → 1/√2, y → 1/√2}}
```

Alternativamente, podemos pensar en dos polinomios en la variable $x$, y calculamos para qué valores de $y$ ambos tienen ceros en común. Entonces ponemos

```
In[100]:= Resultant[x^2+y^2-1,x-y,x]
```

```
Out[100]= -1 + 2y^2
```

y resolvemos

```
In[101]:= Solve[%==0]
```

```
Out[101]= {{y → -1/√2}, {y → 1/√2}}
```

```
In[102]:= {x^2+y^2-1,x-y}/.%
```

```
Out[102]= {{-1/2 + x^2, 1/√2+x}, {-1/2 + x^2, -1/√2+x}}
```

```
In[103]:= Solve[{x^2-1/2==0}]
```

Out[103]= $\{\{x \to -\frac{1}{\sqrt{2}}\}, \{x \to \frac{1}{\sqrt{2}}\}\}$

Ejercicio: Sea $a$ una raiz del polinomio $x^4-3x^3+5x^2+4x-3$ y sea $b = 2a^2-3a+4$. Usando la función resultante, encuentra un polinomio que tenga a $b$ como raíz.

```
In[104]:= Resultant[x^4-3x^3+5x^2+4x-3,2x^2-3x+4-b,x]
```

Out[104]= $1559 - 560b + 19b^2 - 5b^3 + b^4$

- **Discriminante**

  La función `Resultant` nos permite definir la función `Discriminant` que nos calculará el discriminante de un polinomio.

```
In[105]:=Discriminant[p_, x_] := With[{m = Exponent[p, x]},
      Cancel[(-1)^((1/2) m((m - 1)) Resultant[p, D[p,x] x]/Coefficient[p, x, m]]]
```

Ejercicio: Calcular el discriminante de una cúbica principal.

```
In[106]:= Discriminant[x^3+b x+c,x]
```

Out[106]= $-4b^3 - 27c^2$

Ejercicio ¿Para qué valores de $a$ tiene raíces múltiples el polinomio $x^4 - x^3 - x^2 + x + a$?

```
In[107]:= Solve[Discriminant[x^4-x^3-x^2+x+a,x]==0,a]
```

Out[107]= $\{\{a \to 0\}, \{a \to \frac{1}{512}(107 - 51\sqrt{17})\}, \{a \to \frac{1}{512}(107 + 51\sqrt{17})\}\}$

Se propone como ejercicio final encontrar solución a los ejercicios propuestos en la sección 4.10 que puedan ser resueltos utilizando las funciones definidas en esta Práctica.

# Capítulo 5

# Grupos abelianos finitamente generados

## 5.1. Generalidades

Recordemos que un *grupo abeliano* es un conjunto no vacío $G$ junto con una operación interna $+$ verificando

- es asociativa,
- tiene elemento neutro (al que denotaremos por 0),
- todo elemento $g \in G$ tiene inverso (que denotaremos por $-g$, g+(-g)=0=(-g)+g),
- es conmutativa.

A lo largo de este tema usaremos notación aditiva siempre que tratemos con grupos abelianos. Cuando presentemos propiedades que pueden ser dadas indistintamente para grupos no necesariamente abelianos, usaremos notación multiplicativa, y por tanto 1 denotará el elemento neutro y $g^{-1}$ el inverso del elemento $g$.

Dado $G$ un grupo abeliano y $H$ un subgrupo suyo, se puede definir una relación en $G$ de la siguiente forma

$$a \sim_H b, \text{ si } a - b \in H.$$

Vimos en su día que esta relación es de equivalencia. Las clases de equivalencia son

$$[a] = \{b \in G \mid b \sim_H a\} = \{a + h \mid h \in H\} = a + H.$$

La suma de dos clases se puede definir como

$$(a + H) + (b + H) = (a + b) + H,$$

resultando el conjunto cociente $G/H = G/\sim_H$ un grupo abeliano.

Un *morfismo* entre dos grupos abelianos $A$ y $B$ es una aplicación $f : A \to B$ verificando que

$$f(a + a') = f(a) + f(a'),$$

para cualesquiera $a, a' \in A$.

Recuérdese también que el núcleo del morfismo $f$

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

es un subgrupo de $A$, y que la imagen de $f$

$$\mathrm{Im}(f) = \{f(a) \mid a \in A\}$$

es un subgrupo de $B$. Por el teorema de isomorfía, se tiene que

$$A/\ker(f) \cong \mathrm{Im}(f).$$

Un morfismo de grupos $f : A \to B$ es inyectivo si y sólo si $\ker(f) = 0$, y es sobreyectivo si y sólo si $\mathrm{Im}(f) = B$.

Dado un grupo abeliano cualquiera $A$ y un elemento $a \in A$, podemos definir para todo $n \in \mathbb{N}$

$$na = \begin{cases} 0 & \text{si } n = 0, \\ a + (n-1)a & \text{si } n > 0, \\ (-n)(-a) & \text{si } n < 0. \end{cases}$$

Es fácil comprobar que se verifican las siguientes propiedades para cualesquiera $s, t \in \mathbb{Z}$ y $a, b \in A$:

- $(s + t)a = sa + ta$,
- $s(a + b) = sa + sb$,
- $(st)a = s(ta)$,
- $1a = a$,

lo que convierte a $A$ en un $\mathbb{Z}$-módulo.

## 5.2. Grupos cíclicos

**Definición 5.2.1.** El número de elementos de un grupo $G$ (finito o infinito) se llama *orden del grupo*. Lo denotamos por $|G|$.

**Definición 5.2.2.** El *orden de un elemento* $g \in G$ es el mínimo entero positivo $n$ tal que $g^n = 1$ (en notación aditiva esto es $ng = 0$). Si no existe un tal entero (es decir, si para todo entero positivo $n$ se verifica que $g^n \neq 1$), decimos que $g$ tiene *orden infinito*. El orden de un elemento se denota por $o(g)$.

**Definición 5.2.3.** Un grupo $G$ se llama *cíclico* si existe un elemento $a \in G$ tal que $G = \{a^n \mid n \in \mathbb{Z}\}$. Un tal elemento $a$ se llama *generador* de $G$.

Indicamos que $G$ es un grupo cíclico generado por $a$ mediante la notación $G = \langle a \rangle$.

*Ejemplo* 5.2.4. El conjunto $\mathbb{Z}$ de los enteros con la suma ordinaria es cíclico. Ambos 1 y $-1$ son generadores suyos.

*Ejemplo* 5.2.5. El conjunto $\mathbb{Z}_n$ de las clases de restos módulo $n$ con la suma es cíclico. En este caso también 1 y $-1$ son generadores, pero puede tener muchos mas (dependiendo del valor de $n$).

*Ejemplo* 5.2.6. Es cíclico el grupo aditivo $\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$. Por otra parte, 2 no es un generador de $\mathbb{Z}_8$ por que $\langle 2 \rangle = \{0, 2, 4, 6\} \neq \mathbb{Z}_8$.

*Ejemplo* 5.2.7. Es cíclico el grupo multiplicativo $\mathbb{Z}_{10}^{\times} = U(10) = \{1,3,7,9\} = \{3^0, 3^1, 3^3, 3^2\} = \langle 3 \rangle$. También $U(10) = \langle 7 \rangle$.

*Ejemplo* 5.2.8. No es cíclico el grupo multiplicativo $\mathbb{Z}_8^{\times} = U(8) = \{1,3,5,7\}$ porque $\langle 1 \rangle = \{1\} \neq \mathbb{Z}_8^{\times}$, $\langle 3 \rangle = \{1,3\} \neq \mathbb{Z}_8^{\times}$, $\langle 5 \rangle = \{1,5\} \neq \mathbb{Z}_8^{\times}$, $\langle 7 \rangle = \{1,7\} \neq \mathbb{Z}_8^{\times}$.

**Lema 5.2.9.** *Sea $G$ un grupo y sea $a \in G$ un elemento de orden $n$. Entonces $a^k = 1$ si y sólo si $n$ divide a $k$.*

*Demostración.* Supongamos que $k = ln$ para algún entero $l$. Entonces $a^k = (a^n)^l = 1^l = 1$.

Partamos ahora de que $a^k = 1$. Sean $q$ y $r$ enteros tales que $k = qn + r$ con $0 \leq r < n$. Entonces $1 = a^k = a^{qn+r} = a^{qn}a^r = a^r$. Como $a^r = 1$ y $n$ es el mínimo de los enteros que verifican que $a^n = 1$, deducimos que $r$ tiene que ser cero. Por tanto $n$ divide a $k$. □

**Teorema 5.2.10** (Criterio para $a^i = a^j$)**.** *Sea $G$ un grupo y sea $a \in G$.*

- *Si $o(a) = \infty$, todas las potencias de $a$ son elementos distintos del grupo $G$.*
- *Si $o(a) = n$ es finito, entonces $\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ y $a^i = a^j$ si y sólo si $n$ divide a $i - j$.*

*Demostración.* Es suficiente con probar que $a^i = a^j$ si y sólo si $n$ divide a $i - j$. Obsérvese que al ser $G$ un grupo, $a^i = a^j$ si y sólo si $a^i a^{-j} = a^{i-j} = 1$. Como sabemos que $a^k = 1$ si y sólo si $n$ divide a $k$, tenemos lo que queríamos. □

**Corolario 5.2.11.** *Para cualquier $a \in G$ se tiene que $o(a) = |\langle a \rangle|$.*

**Teorema 5.2.12.** *Sea $a$ un elemento de orden $n$ en un grupo $G$ y sea $k$ un entero positivo. Sea $d = \text{m. c. d.}(n,k)$. Entonces $\langle a^k \rangle = \langle a^d \rangle$ y $o(a^k) = n/d$.*

*Demostración.* Para ver que $\langle a^k \rangle = \langle a^d \rangle$, basta con demostrar que $a^k \in \langle a^d \rangle$ y que $a^d \in \langle a^k \rangle$. Como $d = \text{m. c. d.}(n,k)$, $k = dt$ para algún entero $t$. Por tanto $a^k = (a^d)^t \in \langle a^d \rangle$. Por otro lado, también sabemos (identidad de Bézout) que existen enteros $u$ y $v$ tales que $d = un + vk$. Así $a^d = a^{un+vk} = a^{un}a^{vk} = (a^k)^v \in \langle a^k \rangle$.

Veamos por último que $o(a^k) = n/d$. Por el resultado anterior y lo que acabamos de demostrar, esto equivale a probar que $o(a^d) = n/d$. Nótese que $(a^d)^{\frac{n}{d}} = a^n = 1$. Por otro lado, si $t$ es un entero positivo tal que $(a^d)^t = 1$, entonces por el Lema 5.2.9, $n$ divide a $td$, por lo que $n/d$ divide a $t$. De esta forma $n/d$ es el mínimo entero que verifica que $(a^d)^{\frac{n}{d}} = 1$. Por la definición de orden, $o(a^d) = n/d$. □

Con esto es fácil comprobar cuándo dos subgrupos cíclicos de un grupo cíclico finito son iguales si se conocen sus generadores.

**Corolario 5.2.13** (Criterio para $\langle a^i \rangle = \langle a^j \rangle$)**.** *Sea $o(a) = n$. Entonces $\langle a^i \rangle = \langle a^j \rangle$ si y sólo si* $\text{m. c. d.}(n,i) = \text{m. c. d.}(n,j)$.

El teorema anterior también nos permite ver qué elementos de un grupo cíclico generan ese grupo.

**Corolario 5.2.14** (Generadores de grupos cíclicos)**.** *Sea $G = \langle a \rangle$ un grupo cíclico de orden $n$. Entonces $G = \langle a^k \rangle$ si y sólo si* $\text{m. c. d.}(n,k) = 1$.

Particularizando para $\mathbb{Z}_n$ obtenemos lo siguiente.

**Corolario 5.2.15** (Generadores de $\mathbb{Z}_n$)**.** *Una clase $\bar{k} \in \mathbb{Z}_n$ es un generador de $\mathbb{Z}_n$ si y sólo si* $\text{m. c. d.}(n,k) = 1$.

Veamos ahora cómo son todos los subgrupos de un grupo cíclico. El lector verá cierta similitud entre el primer punto y el hecho de que $\mathbb{Z}$ sea un dominio de ideales principales.

**Teorema 5.2.16** (Teorema fundamental de los grupos cíclicos)**.** *1. Todo subgrupo de un grupo cíclico es cíclico.*

2. *Si $|\langle a\rangle| = n$, el orden de cualquier subgrupo cíclico de $\langle a\rangle$ es un divisor de $n$.*

3. *Para cada divisor positivo $k$ de $n$ existe un único subgrupo de orden $k$, a saber $\langle a^{n/k}\rangle$.*

*Demostración.* Sea $H$ un subgrupo de $G$, con $G$ cíclico. Entonces existe $a \in G$ tal que $G = \langle a\rangle$. Si $H \neq \{1\}$, existe $k = \text{mín}\{n \in \mathbb{N} \setminus \{0\} \mid a^n \in H\}$. Veamos que $H = \langle a^k\rangle$. Claramente $\langle a^k\rangle \subseteq H$. Para ver la otra inclusión, sea $b \in H$. Como $H \subseteq G = \langle a\rangle$, existe $n$ entero tal que $b = a^n$. Sean $q$ y $r$ enteros tales que $n = qk + r$ con $0 \leq r < k$. Tenemos así que $a^r = a^n/((a^k)^q)$ pertenece a $H$ por ser éste un subgrupo de $G$. Por la minimalidad de $k$, esto lleva a que $r = 0$, y por tanto $n = kq$. De aquí deducimos que $b = a^n = (a^k)^q \in \langle a^k\rangle$.

Acabamos de ver que todo subgrupo de $\langle a\rangle$ es de la forma $\langle a^k\rangle$. Por el Teorema 5.2.12, $|\langle a^k\rangle| = n/d$ con $d = \text{m. c. d.}(k, n)$. Por tanto, el orden de todo subgrupo de $|a|$ divide a $n$.

Por último, usando una vez más el Teorema 5.2.12, si tomamos $k$ un divisor de $n$, entonces $n/k$ es también un divisor de $n$. De esta forma $\text{m. c. d.}(n, n/k) = n/k$ y $o(a^{\frac{n}{k}}) = n/(n/k) = k$. Éste además es el único subgrupo de orden $k$ de $\langle a\rangle$. □

Este resultado visto en $\mathbb{Z}_n$ queda como sigue.

**Corolario 5.2.17** (Subgrupos de $\mathbb{Z}_n$)**.** *Para cada divisor positivo $k$ de $n$ el conjunto $\langle n/k\rangle$ es el único subgrupo de $\mathbb{Z}_n$ de orden $k$.*

*Estos son los únicos subgrupos de $\mathbb{Z}_n$.*

**Definición 5.2.18.** La función *tociente de Euler* se define como $\phi(1) = 1$ y para todo entero $n > 1$, $\phi(n)$ es el número de enteros positivos menores que $n$ y primos relativos con $n$.

Nótese que $|U(n)| = \phi(n)$.

**Teorema 5.2.19.** *Si $d$ es un divisor positivo de $n$, el número de elementos de orden $d$ en un grupo cíclico de orden $n$ es $\phi(d)$.*

**Corolario 5.2.20.** *En cualquier grupo finito $G$, el número de elementos de orden $d$ es divisible por $\phi(d)$.*

## 5.3. Teorema de Lagrange

Acabamos de ver que el orden de todo subgrupo de un grupo cíclico divide al orden del grupo cíclico. Esta propiedad es cierta para cualquier subgrupo de un grupo cualquiera. Nosotros vamos a probar ese hecho para grupos finitos. Sea $G$ un grupo finito y $H$ un subgrupo suyo. Definimos en $G$ la relación $a \sim_H b$ si $ab^{-1} \in H$ (usando notación multiplicativa). Es fácil demostrar que por ser $H$ un subgrupo de $G$, esa relación es una relación de equivalencia. Sus clases $[a] = \{b \in G \mid a \sim_H b\}$ son de la forma $[a] = aH$, ya que $ab^{-1} = h \in H$ lleva a $b = ah^{-1} \in aH$. De esta forma

$$G = \bigcup_{a \in G} aH,$$

y si $a_1H, \ldots, a_kH$ son las distintas clases de equivalencia de $\sim_H$, entonces

$$G = \bigcup_{i=1}^{k} a_iH$$

y esa unión es disjunta. Por otro lado, es fácil ver que el cardinal de $aH$ es igual que el cardinal de $H$ para todo $a \in G$. De esta forma obtenemos que el cardinal de $G$ es $k$ veces el de $H$.

**Teorema 5.3.1.** *Sea $G$ un grupo finito y $H$ un subgrupo suyo. Entonces $|H|$ divide a $|G|$.*

Nótese que si $G$ es abeliano, entonces el cociente $G/\sim_H = G/H$ es un grupo abeliano, y lo que obtenemos es que

$$|G| = |G/H| \cdot |H|.$$

## 5.4. Sumas directas

**Definición 5.4.1.** Sean $M_1, \ldots, M_n$ una colección finita de grupos abelianos (notados aditivamente). La *suma directa externa* de los $M_j$ es el conjunto producto cartesiano,

$$M_1 \times \cdots \times M_n = \{(x_1, \ldots, x_n) \mid x_j \in M_j\}$$

con la suma definida por componentes:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

El siguiente resultado es fácil de probar.

**Proposición 5.4.2.** *La suma directa externa de grupos abelianos es un grupo abeliano.*

Si $M$ y $N$ son subgrupos de $A$, entonces tanto $M + N = \{m + n \mid m \in M, n \in N\}$ como $M \cap N$ son de nuevo subgrupos de $A$.

**Definición 5.4.3.** Sean $M$ y $N$ dos subgrupos de $A$. Decimos que $A$ es *suma directa* de $M$ y $N$ si

- $M + N = A$,
- $M \cap N = \{0\}$.

Este hecho lo denotaremos por $A = M \oplus N$.

**Teorema 5.4.4.** *Supongamos que $A = M \oplus N$. Entonces todo elemento de a de A se escribe de forma única como $a = m + n$ con $m \in M$ y $n \in N$. Además, la aplicación*

$$M \times N \to M \oplus N,\ (m, n) \mapsto m + n$$

*es un isomorfismo de grupos.*

*Demostración.* Esta aplicación es un morfismo (lo cual es fácil de probar). Además por ser $A = M + N$, esta aplicación es sobreyectiva. Veamos que es inyectiva, y para eso comprobemos que su núcleo es cero. Sea $(m, n)$ tal que $m + n = 0$. Entonces $m = -n$ está en $M$ y en $N$ a la vez. Como $M \cap N = \{0\}$, esto lleva a $m = n = 0$ y $(m, n) = (0, 0)$. □

Podemos por tanto a partir de ahora identificar $M \oplus N$ con $M \times N$.

*Ejemplo* 5.4.5. $U(8) \times U(10)$.

*Ejemplo* 5.4.6. $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$. Nótese que $\mathbb{Z}_6 = \langle 3 \rangle \oplus \langle 2 \rangle = \{0, 3\} \oplus \{0, 2, 4\} \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

**Teorema 5.4.7.** *El orden de un elemento en una suma directa de un número finito de grupos abelianos finitos es el mínimo común múltiplo de los órdenes de sus componentes, es decir*

$$o((x_1, \ldots, x_n)) = \text{m. c. m.}(o(x_1), \ldots, o(x_n))$$

*Demostración.* Si $k(x_1, \ldots, x_n) = 0$, entonces $kx_1 = 0$, $kx_2 = 0, \ldots, kx_n = 0$. Por tanto $k$ es un múltiplo de los órdenes de $x_1, x_2, \ldots, x_n$. Con esta observación es fácil demostrar el resultado deseado. □

*Ejemplo* 5.4.8. Determinación de los elementos de orden 5 en $\mathbb{Z}_{25} \times \mathbb{Z}_5$. Sea $(x, y) \in \mathbb{Z}_{25} \times \mathbb{Z}_5$. Como $o(x, y) = \text{m. c. m.}(o(x), o(y))$, si $o(x, y) = 5$, entonces $\{o(x), o(y)\} \subseteq \{1, 5\}$. El único elemento de orden uno es el cero. Los elementos de orden cinco de $\mathbb{Z}_5$ están en el conjunto $A = \{1, 2, 3, 4\}$, y los de $\mathbb{Z}_{25}$ están en $B = \mathbb{Z}_{25} \setminus \{0, 5, 10, 15, 20\}$. Así los elementos de orden cinco en $\mathbb{Z}_{25} \times \mathbb{Z}_5$, son de la forma

- $(0, b)$ con $b \in B$,
- $(a, 0)$ con $a \in A$,
- $(a, b)$ con $a \in A$ y $b \in B$.

*Ejemplo* 5.4.9. Determinación del número de subgrupos de orden 10 en $\mathbb{Z}_{100} \times \mathbb{Z}_{25}$.

*Ejemplo* 5.4.10. Orden del subgrupo $\langle 5 \rangle \times \langle 3 \rangle \subset \mathbb{Z}_{30} \times \mathbb{Z}_{12}$.

**Teorema 5.4.11** (Criterio para que $G \times H$ sea cíclico)**.** *Sean $G$ y $H$ grupos cíclicos finitos. Entonces $G \times H$ es cíclico si y sólo si* $\text{m. c. d.}(|G|, |H|) = 1$.

*Demostración.* Supongamos que $G = \langle a \rangle$ y que $H = \langle b = \rangle$. Sean $n = o(a) = |G|$ y $m = o(b) = |H|$.

Si $\text{m. c. d.}(n, m) = 1$, entonces $\text{m. c. m.}(n, m) = nm$ y por tanto el elemento $(a, b)$ tiene orden $nm$ en virtud del Teorema 5.4.7. Como $|G \times H| = n \times m$, esto lleva que el grupo cíclico generado por $(a, b)$ es todo $G \times H$.

Si $G \times H$ es cíclico, entonces existe $(x, y) \in G \times H$ de forma que $\langle (x, y) \rangle = G \times H$. Por tanto el orden de $(x, y)$ es $nm$. Como $o((x, y)) = \text{m. c. m.}(o(x), o(y)) = nm$, y además el orden de $x$ divide a $n$ y el de $y$ a $m$, se tiene que $o(x) = n$, $o(y) = m$ y $\text{m. c. d.}(n, m) = 1$. □

**Corolario 5.4.12.** *Una suma directa externa $M_1 \times \cdots \times M_n$ es un grupo cíclico si y sólo si los $M_j$ son cíclicos finitos y para todo par $i \neq j$ se verifica que* $\text{m. c. m.}(|M_i|, |M_j|) = 1$.

**Corolario 5.4.13** (Teorema chino del resto)**.** *Sea $m = n_1 \dots n_k$ un entero positivo. Entonces $\mathbb{Z}_m \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ si y sólo si para todo par $i \neq j$ los enteros $n_i$ y $n_j$ son primos relativos.*

*Ejemplo* 5.4.14. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{15} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_5 \ncong \mathbb{Z}_{60} \cong \mathbb{Z}_4 \times \mathbb{Z}_{15}$.

**Definición 5.4.15.** Para $k \mid n$ definimos

$$U_k(n) = \{x \in U(n) \mid x \equiv 1 \pmod{k}\}$$

**Teorema 5.4.16.** *Sean $s, t$ enteros positivos primos relativos. Entonces*

$$\begin{aligned} U(st) &\cong U(s) \times U(t) \\ U_s(st) &\cong U(t) \\ U_t(st) &\cong U(s) \end{aligned}$$

**Corolario 5.4.17.** *Sea $m = n_1 \dots n_k$ un entero positivo tal que* $\text{m. c. d.}(n_i, n_j) = 1$ *para todo par $i \neq j$. Entonces*

$$U(m) \cong U(n_1) \times \cdots \times U(n_k)$$

*Ejemplo* 5.4.18. $U(105)$.

## 5.5. Grupos abelianos libres

Sea $A$ un grupo abeliano y sean $a_1, \dots, a_s \in A$ elementos suyos.

**Definición 5.5.1.** Decimos que $A$ está generado por $a_1, \dots, a_s$, o bien que $\{a_1, \dots, a_s\}$ es un *sistema de generadores* de $A$, si todo $a \in A$ se expresa como

$$a = k_1 a_1 + \cdots + k_s a_s$$

con $k_1, \ldots, k_s \in \mathbb{Z}$, a saber,

$$A = \langle a_1, \ldots, a_s \rangle.$$

El grupo $A$ se llama *abeliano libre sobre* $a_1, \ldots, a_s$ si todo elemento $a \in A$ se expresa de manera única como

$$a = k_1 a_1 + \cdots + k_s a_s$$

con $k_1, \ldots, k_s \in \mathbb{Z}$.

Si este es el caso, el conjunto $B = \{a_1, \ldots, a_s\}$ se llama *base de* $A$.

*Ejemplo* 5.5.2. El grupo $A = \mathbb{Z}^s = \mathbb{Z} \times \cdots \times \mathbb{Z}$ es libre sobre $e_1, \ldots e_s$, siendo $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (un 1 en la posición $i$ y 0 en todas las demás).

*Ejemplo* 5.5.3. Si $A$ es libre sobre $\{a_1, \ldots, a_s\}$ y $B$ es libre sobre $\{b_1, \ldots, b_t\}$, entonces $A \times B$ es libre sobre $\{(a_1, 0), \ldots, (a_s, 0), (0, b_1), \ldots, (0, b_t)\}$.

**Proposición 5.5.4.** *Sea $A$ un grupo abeliano libre sobre $a_1, \ldots, a_s$. Entonces existe un isomorfismo $f : \mathbb{Z}^s \cong A$ dado por $f(e_i) = a_i$, $i = 1, \ldots, s$.*

*Demostración.* Sea $B = \{a_1, \ldots, a_s\}$. Defínase $f(z_1, \ldots, z_s) = z_1 a_1 + \cdots + z_s a_s$. Por la definición de base, obtenemos que $f$ es sobreyectiva (todo elemento se expresa como combinación de los elementos de $B$) e inyectiva (la expresión de un elemento es única). □

**Teorema 5.5.5** (Propiedad universal del grupo abeliano libre)**.** *Sea $F$ un grupo abeliano libre sobre $B = \{a_1, \ldots, a_s\}$. Para cualquier grupo abeliano $A$ y cualquier aplicación $f : B \to A$ existe un único homomorfismo de grupos $\overline{f} : F \to A$ tal que $\overline{f}(a_i) = f(a_i)$, $i = 1, \ldots, s$.*

*Demostración.* Todo elemento $a \in F$ se escribe de forma única como $a = \lambda_1 z_1 + \cdots + \lambda_n z_n$. Podemos definir $\overline{f}(a) = \lambda_1 f(a_1) + \cdots + \lambda_n f(a_n)$. Compruébese que es un homomorfismo de grupos.

Si $g : F \to A$ es un homomorfismo de grupos tal que $g(a_i) = f(a_i)$, entonces para cualquier $a = \lambda_1 z_1 + \cdots + \lambda_n z_n \in F$, se tiene que

$$g(a) = g(\lambda_1 z_1 + \cdots + \lambda_n z_n) = \lambda_1 g(a_1) + \cdots + \lambda_n g(a_n) = \lambda_1 f(a_1) + \cdots + \lambda_n f(a_n) = \overline{f}(a).$$

De aquí deducimos que $g = \overline{f}$. □

**Corolario 5.5.6.** *Todo grupo abeliano finitamente generado es isomorfo a un grupo cociente de un grupo abeliano libre.*

*Demostración.* Sea $G = \langle a_1, \ldots, a_n \rangle$. Sea $f : \mathbb{Z}^n \to G$ el morfismo que viene determinado por $f(e_i) = a_i$, $i \in \{1, \ldots, n\}$. Claramente $f$ es sobreyectiva, y por el teorema de isomorfía, $\mathbb{Z}^n / \ker(f) \cong G$. □

Todo subgrupo de un grupo libre es libre. Para probar este hecho tenemos que introducir una nueva herramienta: las sucesiones exactas cortas.

## 5.6. Secuencias exactas cortas

Sean $A$, $B$ y $C$ tres grupos abelianos, y $f : A \to B$ y $g : B \to C$ dos morfismos de grupos. Decimos que la secuencia $\{f, g\}$ es una *secuencia exacta corta* si

1. $f$ es inyectiva,
2. $g$ es sobreyectiva y

3. $\mathrm{Im}(f) = \ker(g)$.

Normalmente expresaremos que $\{f, g\}$ es una secuencia exacta corta escribiendo

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

La secuencia exacta corta $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *escinde* si existe $h : C \to B$ tal que $g \circ h = Id$.

**Teorema 5.6.1.** *Si la secuencia exacta corta* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *escinde, entonces* $B \cong A \times C$.

*Demostración.* Sea $h : C \to B$ tal que $g \circ h = Id$. Tomamos $k : A \times C \to B$ la aplicación $k(a, c) = f(a) + h(c)$. Esta aplicación es claramente un morfismo de grupos. Si $k(a, c) = 0$, entonces $-f(a) = h(c)$. Pero eso lleva a $g(-f(a)) = -g(f(a)) = g(h(c))$. Como $\ker(g) = \mathrm{Im}(f)$ y $g \circ h = Id$, $g(f(a)) = 0$ y en consecuencia $c = g(h(c)) = 0$. Así $0 = k(a, c) = f(a) + h(c) = f(a) + h(0) = f(a)$. Usando que $f$ es inyectiva, concluimos que $a = 0$. De esta forma $k(a, c) = 0$ implica que $(a, c) = (0, 0)$. Veamos que $k$ es sobreyectiva. Sea $b \in B$. Entonces $g(b - h(g(b))) = g(b) - g(h(g(b))) = g(b) - Id(g(b)) = 0$. Por tanto $b - h(g(b)) \in \ker(g) = \mathrm{Im}(f)$, por lo que existe $a \in A$ tal que $f(a) = g - h(g(b))$. De esta forma $k(a, g(b)) = b$, lo que prueba que $k$ es sobre. □

Obsérvese que la sucesión $0 \to A \xrightarrow{i_1} A \times C \xrightarrow{\pi_2} C \to 0$, con $i_i(a) = (a, 0)$ y $\pi_2(a, c) = c$, siempre escinde.

**Proposición 5.6.2.** *Toda sucesión exacta corta* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$, *con* $C$ *libre sobre un conjunto finito, escinde.*

*Demostración.* Sea $\{c_1, \ldots, c_s\}$ una base de $C$. Como $g$ es sobreyectiva, para cada $i \in \{1, \ldots, s\}$ existe $b_i \in B$ tal que $g(b_i) = c_i$. Sea $h : C \to B$ el morfismo determinado por $h(c_i) = b_i$. Como $g \circ h(c_i) = c_i = Id(c_i)$ para todo $i$, se tiene que $g \circ h = Id$. □

**Teorema 5.6.3.** *Todo subgrupo de un grupo abeliano libre de rango finito es libre.*

*Demostración.* Basta probar que todo subgrupo de $\mathbb{Z}^n$ es libre, ya que todo grupo libre de rango finito es isomorfo a $\mathbb{Z}^n$ para algún entero positivo $n$. Procedemos por inducción sobre $n$.

Si $n = 1$, sabemos que todo subgrupo $G$ de $\mathbb{Z}$ es un ideal suyo y por tanto es principal ($\mathbb{Z}$ es un dominio de ideales principales). De esta forma $G = \langle g \rangle$, y claramente $G$ es libre.

Supongamos que el resultado es cierto para los subgrupos de $\mathbb{Z}^{n-1}$, y probémoslo para subgrupos de $\mathbb{Z}^n$. Consideramos la sucesión exacta corta

$$0 \to \mathbb{Z}^{n-1} \xrightarrow{i} \mathbb{Z}^n \xrightarrow{\pi} \mathbb{Z} \to 0,$$

con $i$ la inclusión y $\pi$ la proyección en la última coordenada. Esta sucesión induce otra

$$0 \to A \cap \mathbb{Z}^{n-1} \xrightarrow{i} A \xrightarrow{\pi} \pi(A) \to 0.$$

Pueden ocurrir dos cosas.

- Que $\pi(A)$ se cero, con lo que $A$ es un subgrupo de $\mathbb{Z}^{n-1}$ y el resultado queda probado por inducción.
- Que $\pi(A)$ no sea cero. Al ser un subgrupo $\mathbb{Z}$, es libre y por tanto la secuencia escinde, lo que lleva a $A \cong A \cap \mathbb{Z}^{n-1} \times \pi(A)$. Como por hipótesis de inducción $A \cap \mathbb{Z}^{n-1}$ es libre y $\pi(A)$ también lo es, concluimos que $A$ es libre.

□

## 5.7. Matrices de cambio de base

Sea $F$ un grupo abeliano libre de rango $n$ y sean

$$\mathcal{B} = \{e_1, \ldots, e_n\}, \qquad \mathcal{B}' = \{e'_1, \ldots, e'_n\}$$

dos bases suyas. Los elementos de cada una se expresan de manera única como combinación lineal de los elementos de la otra con coeficientes enteros:

$$e'_j = \sum_{i=1}^{n} p_{ij} e_i, \qquad e_i = \sum_{j=1}^{n} \bar{p}_{ji} e'_j$$

Formamos las matrices

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \cdots & \cdots & \cdots \\ p_{n1} & \cdots & p_{nn} \end{pmatrix}, \qquad \bar{P} = \begin{pmatrix} \bar{p}_{11} & \cdots & \bar{p}_{1n} \\ \cdots & \cdots & \cdots \\ \bar{p}_{n1} & \cdots & \bar{p}_{nn} \end{pmatrix}$$

Un cálculo simple muestra que $P\bar{P} = I = \bar{P}P$, así que la matriz $P$ es invertible en $M_{n\times n}(\mathbb{Z})$ y de hecho $\bar{P} = P^{-1}$

Un elemento arbitrario $x \in F$ se expresa de manera única como combinación de los elementos de cada una de las bases con coeficientes enteros:

$$x = \sum_i x_i e_i = \sum_j x'_j e'_j = \sum_j x'_j \sum_i p_{ij} e_i = \sum_i \left( \sum_j x'_j p_{ij} \right) e_i$$

de donde

$$\forall i = 1, \ldots, n \quad x_i = \sum_j p_{ij} x'_j$$

De manera análoga se ve que

$$\forall j = 1, \ldots, n \quad x'_j = \sum_i \bar{p}_{ji} x_i$$

En forma matricial estas igualdades se expresan como

$$\begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \cdots & \cdots & \cdots \\ p_{n1} & \cdots & p_{nn} \end{pmatrix} \begin{pmatrix} x'_1 \\ \cdots \\ x'_n \end{pmatrix}, \qquad \begin{pmatrix} x'_1 \\ \cdots \\ x'_n \end{pmatrix} = \begin{pmatrix} \bar{p}_{11} & \cdots & \bar{p}_{1n} \\ \cdots & \cdots & \cdots \\ \bar{p}_{n1} & \cdots & \bar{p}_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}$$

Llamando $X = (x_1, \ldots, x_n)^T$, $X' = (x'_1, \ldots, x'_n)^T$ (vectores columna) obtenemos la forma compacta

$$X = PX', \qquad X' = P^{-1}X$$

## 5.8. Matrices de homomorfismos

Sean $F_1$ y $F_2$ dos grupos abelianos libres, con bases respectivas

$$\mathcal{B}_1 = \{f_1, \ldots, f_n\}, \qquad \mathcal{B}_2 = \{e_1, \ldots, e_m\}$$

Sea $\varphi : F_1 \to F_2$ un homomorfismo de grupos abelianos. La imagen de cada elemento $f_j$ se expresa de manera única como combinación lineal de los elementos $e_i$:

$$\varphi(f_j) = a_{1j}e_1 + \ldots a_{mj}e_m = \sum_{i=1}^{m} a_{ij}e_i$$

Un elemento arbitrario $y \in F_1$ se expresa de manera única como

$$y = y_1f_1 + \cdots + y_nf_n = \sum_{j=1}^{n} y_jf_j$$

Su imagen bajo $\varphi$ es

$$\varphi(y) = \varphi\left(\sum_{j=1}^{n} y_jf_j\right) = \sum_{j=1}^{n} y_j\varphi(f_j) = \sum_{j=1}^{n} y_j \sum_{i=1}^{m} a_{ij}e_i = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_{ij}y_j\right)e_i = \sum_{i=1}^{m} x_ie_i$$

de donde las coordenadas de $\varphi(y)$ respecto a la base $\mathcal{B}_2$ son $x_i = \sum_j a_{ij}y_j$. Usando las matrices

$$X = \begin{pmatrix} x_1 \\ \ldots \\ x_m \end{pmatrix}, \qquad A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}, \qquad Y = \begin{pmatrix} y_1 \\ \ldots \\ y_n \end{pmatrix}$$

podemos escribir de forma compacta:

$$X = AY$$

Sean ahora

$$\mathcal{B}_1' = \{f_1', \ldots, f_n'\}, \qquad \mathcal{B}_2' = \{e_1', \ldots, e_m'\}$$

otras dos bases respectivas de $F_1$ y $F_2$. Sea $P$ la matriz de cambio de base en $F_2$ y sea $Q$ la matriz de cambio de base en $F_1$. Es decir, que para vectores respectivos se tiene

$$X = PX', \qquad Y = QY'$$

La matriz $A'$ que corresponde a $\varphi$ respecto a las nuevas bases verifica $X' = A'Y'$, pero

$$X' = P^{-1}X = P^{-1}AY = P^{-1}AQY'$$

así que

$$A' = P^{-1}AQ$$

**Teorema 5.8.1.** *Sea $n$ un entero positivo y $f : \mathbb{Z}^n \to \mathbb{Z}^n$ un morfismo de grupos definido por $f(x) = Ax$, con $A$ una matriz de entradas enteras. Si $f$ es sobreyectiva, entonces $A$ tiene inverso (esto implica en particular que $f$ es un isomorfismo).*

*Demostración.* Como $f$ es sobreyectiva, sean $c_1, \ldots, c_n \in \mathbb{Z}^n$ tales que $Ac_i = e_i$. La matriz $C$ cuyas columnas son $c_1, \ldots, c_n$ es la inversa de $A$, ya que $AC = Id$. □

**Corolario 5.8.2.** *Sean $n$ y $m$ enteros positivos y $f : \mathbb{Z}^n \to \mathbb{Z}^m$ un epimorfismo de grupos. Entonces $n \geq m$.*

*Demostración.* Supongamos por el contrario que $n < m$. Sea $k \in \mathbb{N} \setminus \{0\}$ tal que $n + k = m$. Definimos $h : \mathbb{Z}^m = \mathbb{Z}^n \times \mathbb{Z}^k \to \mathbb{Z}^m$ como $h(a, b) = f(a)$. Como $f$ es un epimorfismo, entonces también lo es $h$. Por el teorema anterior, tenemos que $h$ tiene que ser un isomorfismo. Pero esto es imposible, ya que $h(0, b) = 0$ para todo $b \in \mathbb{Z}^k$ y por tanto no puede ser inyectiva. □

**Corolario 5.8.3.** *Dos bases distintas (y finitas) del mismo grupo abeliano libre tienen el mismo número de elementos.*

Si $A$ es un grupo abeliano libre sobre $a_1, \ldots, a_s$, a $s$ se le conoce como el *rango de $A$*.

## 5.9. Equivalencia de matrices en $\mathbb{Z}$

**Definición 5.9.1.** Dos matrices $A, B \in M_{m\times n}(\mathbb{Z})$ se llaman *equivalentes* si existen matrices invertibles $P \in M_m(\mathbb{Z})$, $Q \in M_n(\mathbb{Z})$ tales que $B = PAQ$.

**Lema 5.9.2.** *La relación anterior es una relación de equivalencia en $M_{m\times n}(\mathbb{Z})$.*

El problema que consideramos es seleccionar entre las matrices equivalentes a una matriz $A$ dada, una que tenga una forma "normal" sencilla.

Vamos a obtener las matrices $P, Q$ que transforman $A$ en una matriz en forma normal como producto de matrices de unos tipos especiales que definimos ahora:

Llamamos $e_{ij}$ a la matriz con coeficiente 1 en el lugar $(i, j)$ y 0 en todos los demás. Llamamos $I$ a la matriz identidad.

Obsérvese que $I = e_{11} + \cdots + e_{ii} + \ldots$.

**Definición 5.9.3.** Una *matriz elemental* es una matriz cuadrada de uno de los siguientes tipos:

1. Para todo $b \in \mathbb{Z}$ y todo par de índices $i \neq j$ la matriz
$$T_{ij}(b) = I + be_{ij}$$
se llama *matriz elemental de tipo I*.
2. Para $u = \pm 1$ y todo índice $i$, la matriz
$$D_i(u) = I + (u - 1)e_{ii}$$
se llama *matriz elemental de tipo II*.
3. Para todo par de índices $i \neq j$, la matriz
$$P_{ij} = I - e_{ii} - e_{jj} + e_{ij} + e_{ji}$$
se llama *matriz elemental de tipo III*.

**Lema 5.9.4.** *Las matrices elementales son invertibles. Explícitamente,*
$$T_{ij}(b)^{-1} = T_{ij}(-b), \qquad D_i(u)^{-1} = D_i(u), \qquad P_{ij}^{-1} = P_{ij}$$

**Definición 5.9.5.** La multiplicación por la izquierda de una matriz $A$ por una matriz elemental de tipo I (II, III) se llama *transformación elemental por filas de tipo I (II, III)* de la matriz $A$.

La multiplicación por la derecha de una matriz $A$ por una matriz elemental de tipo I (II, III) se llama *transformación elemental por columnas de tipo I (II, III)* de la matriz $A$.

Sea una matriz $m \times n$.
$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$$

**Lema 5.9.6.** *1. Una transformación elemental por filas de tipo I sustituye $A$ por la matriz*
$$A' = T_{ij}(b)A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a'_{i1} & \ldots & a'_{in} \\ \ldots & \ldots & \ldots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$$
*donde $a'_{ik} = a_{ik} + ba_{jk}$ para $k = 1, \ldots n$*

2. *Una transformación elemental por filas de tipo II sustituye A por la matriz*

$$A' = D_i(u)A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a'_{i1} & \dots & a'_{in} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

*donde* $a'_{ik} = ua_{ik}$ *para* $k = 1, \dots n$

3. *Una transformación elemental por filas de tipo III sustituye A por la matriz*

$$A' = P_{ij}A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a'_{i1} & \dots & a'_{in} \\ \dots & \dots & \dots \\ a'_{j1} & \dots & a'_{jn} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

*donde* $a'_{ik} = a_{jk}$ *y* $a'_{jk} = a_{ik}$ *para* $k = 1, \dots n$

**Lema 5.9.7.** 1. *Una transformación elemental por columnas de tipo I sustituye A por la matriz*

$$A' = AT_{ij}(b) = \begin{pmatrix} a_{11} & \dots & a'_{1j} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a'_{mj} & \dots & a_{mn} \end{pmatrix}$$

*donde* $a'_{kj} = a_{kj} + ba_{ki}$ *para* $k = 1, \dots m$

2. *Una transformación elemental por columnas de tipo II sustituye A por la matriz*

$$A' = AD_i(u) = \begin{pmatrix} a_{11} & \dots & a'_{1i} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a'_{mi} & \dots & a_{mn} \end{pmatrix}$$

*donde* $a'_{ki} = ua_{ki}$ *para* $k = 1, \dots m$

3. *Una transformación elemental por columnas de tipo III sustituye A por la matriz*

$$A' = AP_{ij} = \begin{pmatrix} a_{11} & \dots & a'_{1i} & \dots & a'_{1j} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a'_{mi} & \dots & a'_{mj} & \dots & a_{mn} \end{pmatrix}$$

*donde* $a'_{ki} = a_{kj}$ *y* $a'_{kj} = a_{ki}$ *para* $k = 1, \dots m$

**Lema 5.9.8.** *Las matrices que se obtienen a partir de A por transformaciones elementales de filas o columnas son equivalentes a la matriz A.*

**Proposición 5.9.9.** *Sea A una matriz* $m \times n$ *con coeficientes enteros. Existen matrices* $P_0, Q_0$ *invertibles sobre* $\mathbb{Z}$ *de órdenes respectivos* $m, n$ *tales que*

$$P_0MQ_0 = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & b_{m2} & \dots & b_{mn} \end{pmatrix}$$

*donde* $d_1 \geq 0$ *y* $d_1 \mid b_{ij}$ *para todo par i, j.*

*Demostración.* Si $A = 0$ es la matriz cero, no hay nada que demostrar.

Si $A \neq 0$, sea $a_{ij}$ un elemento no nulo con valor absoluto mínimo. Mediante transformaciones elementales de filas y columnas podemos llevar este elemento a la posición $(1,1)$.

Suponemos que ya está ahí. Si $a_{11} < 0$, cambiamos de signo toda la primera columna (transformación elemental de tipo II). Sea $k > 1$ y sea $a_{1k} = a_{11}b_k + b_{1k}$ con $0 \leq b_{1k} < |a_{ij}|$. Restamos la primera columna multiplicada por $b_k$ de la $k$-ésima. Esta transformación elemental reemplaza $a_{1k}$ por $b_{1k}$. Si $b_{1k} \neq 0$ obtenemos una matriz equivalente a la matriz $A$ para la que el mínimo de los valores absolutos de los coeficientes no nulos es estrictamente menor que el de $A$. Repetimos el procedimiento original con esta matriz.

De la misma forma, si $a_{k1} = a_{11}b_k + b_{k1}$ con $0 < b_{k1} < |a11|$, una transformación elemental por filas de tipo I proporciona una matriz equivalente para la que el mínimo de los valores absolutos de los coeficientes es estrictamente menor que el de $A$. Ya que cada aplicación de este proceso disminuye dicho mínimo, un número finito de repeticiones nos lleva a una matriz $B = (b_{ij})$ equivalente con $A$ tal que $b_{11}$ divide a todos los $b_{1k}$ y todos los $b_{k1}$. Nuevas transformaciones elementales de tipo I de filas y de columnas da una matriz equivalente con $A$ de la forma

$$\begin{pmatrix} b_{11} & 0 & \dots & 0 \\ 0 & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & c_{m2} & \dots & c_{mn} \end{pmatrix}$$

Si existe un $c_{ij}$ no divisible por $b_{11}$, sumamos la $i$-ésima fila a la primera con lo que obtenemos la nueva primera fila $(b_{11}, c_{i2}, \dots, c_{in})$ con $b_{11} \nmid c_{ij}$. Repitiendo el primer proceso reemplazamos $c_{ij}$ por un entero positivo menor que $|b_{11}|$.

Un número finito de pasos como los indicados darán finalmente la matriz buscada. □

**Teorema 5.9.10** (Forma normal de Smith para matrices enteras)**.** *Sea $A$ una matriz $m \times n$ con coeficientes enteros. Existen matrices $P, Q$ invertibles sobre $\mathbb{Z}$ de órdenes respectivos $m, n$ tales que*

$$PAQ = \begin{pmatrix} d_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & d_r & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 \end{pmatrix}$$

*donde $d_i > 0$ y $d_i \mid d_{i+1}$ para todo $i$.*

*Demostración.* Inducción sobre el número de filas y columnas. Dada una matriz $A \in M_{m\times n}(\mathbb{Z})$, la proposición 5.9.9 genera una matriz equivalente

$$\begin{pmatrix} d_1 & 0 \\ 0 & A_1 \end{pmatrix}$$

donde $A_1 \in M_{(m-1)\times(n-1)}(\mathbb{Z})$ y todos los coeficientes de $A_1$ son divisibles por $d_1$. Por inducción, transformaciones elementales de filas y columnas transforman $A_1$ a una matriz

$$\begin{pmatrix} d_2 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & d_r & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix}$$

con $d_i \mid d_{i+1}$. □

**Definición 5.9.11.** El número $r$ de elementos no nulos en la diagonal de la forma normal de Smith de una matriz $A$ se llama *rango de* $A$.

Los elementos no nulos $d_i$ en la diagonal se llaman *factores invariantes de la matriz* $A$.

**Teorema 5.9.12.** *Sea $A \in M_{m\times n}(\mathbb{Z})$ de rango $r$. Para cada $i = 1, \dots r$ sea $\Delta_i$ el máximo común divisor de los menores $i \times i$ de $A$. Entonces los factores invariantes de $A$ son*

$$d_1 = \Delta_1, \quad d_2 = \Delta_2/\Delta_1, \quad \dots \quad d_r = \Delta_r/\Delta_{r-1}$$

**Corolario 5.9.13.** *Los factores invariantes $d_i$ del teorema 5.9.10 están determinados de manera única por la matriz $A$.*

**Corolario 5.9.14.** *Dos matrices $A, B \in M_{m\times n}(\mathbb{Z})$ son equivalentes si y sólo si tienen los mismos factores invariantes.*

*Observación* 5.9.15. El teorema 5.9.10 fue demostrado en 1861 por H. J. S. Smith. Anteriormente Gauss y otros habían utilizado la reducción $A \to AQ$ en un cuerpo para obtener la forma escalonada sobre un cuerpo (en álgebra lineal se estudia como método del pivote, eliminación de Gauss, forma normal de Hermite). Mas reciente es la extensión a matrices con coeficientes en un dominio de ideales principales. (En el siguiente tema la veremos sólo para dominios euclídeos).

*Ejemplo* 5.9.16. Para ilustrar los procedimientos anteriores tomamos un ejemplo sencillo y realizamos paso a paso las reducciones. Sea la matriz

$$A = \begin{pmatrix} 2 & 3 & 2 \\ 1 & 6 & 4 \\ 3 & -2 & 4 \end{pmatrix}$$

Queremos reducirla a su forma normal de Smith. Desarrollamos el trabajo en forma tabular arrastrando los productos de transformaciones de filas a la izquierda y los productos de transformaciones de columnas a la derecha. La columna central empieza con $A$ y termina con $D$, la forma normal de Smith:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 2 | 3 | 2 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 6 | 4 | 0 | 1 | 0 |
| 0 | 0 | 1 | 3 | −2 | 4 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 | 6 | 4 | | | |
| 1 | 0 | 0 | 2 | 3 | 2 | | | |
| 0 | 0 | 1 | 3 | −2 | 4 | | | |
| 0 | 1 | 0 | 1 | 6 | 4 | | | |
| 1 | −2 | 0 | 0 | −9 | −6 | | | |
| 0 | 0 | 1 | 3 | −2 | 4 | | | |
| 0 | 1 | 0 | 1 | 6 | 4 | | | |
| 1 | −2 | 0 | 0 | −9 | −6 | | | |
| 0 | −3 | 1 | 0 | −20 | −8 | | | |
| | | | 1 | 0 | 4 | 1 | −6 | 0 |
| | | | 0 | −9 | −6 | 0 | 1 | 0 |
| | | | 0 | −20 | −8 | 0 | 0 | 1 |
| | | | 1 | 0 | 0 | 1 | −6 | −4 |
| | | | 0 | −9 | −6 | 0 | 1 | 0 |
| | | | 0 | −20 | −8 | 0 | 0 | 1 |
| | | | 1 | 0 | 0 | 1 | −4 | −6 |
| | | | 0 | −6 | −9 | 0 | 0 | 1 |
| | | | 0 | −8 | −20 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 0 | 0 | | | |
| 1 | 1 | −1 | 0 | 2 | 11 | | | |
| 0 | −3 | 1 | 0 | −8 | −20 | | | |
| | | | 1 | 0 | 0 | 1 | −4 | 14 |
| | | | 0 | 2 | 1 | 0 | 0 | 1 |
| | | | 0 | −8 | 20 | 0 | 1 | −5 |
| | | | 1 | 0 | 0 | 1 | 14 | −4 |
| | | | 0 | 1 | 2 | 0 | 1 | 0 |
| | | | 0 | 20 | −8 | 0 | −5 | 1 |
| | | | 1 | 0 | 0 | 1 | 14 | −32 |
| | | | 0 | 1 | 0 | 0 | 1 | −2 |
| | | | 0 | 20 | −48 | 0 | −5 | 11 |
| 0 | 1 | 0 | 1 | 0 | 0 | | | |
| 1 | 1 | −1 | 0 | 1 | 0 | | | |
| −20 | −23 | 21 | 0 | 0 | −48 | | | |
| 0 | 1 | 0 | 1 | 0 | 0 | | | |
| 1 | 1 | −1 | 0 | 1 | 0 | | | |
| 20 | 23 | −21 | 0 | 0 | 48 | | | |

Los cálculos anteriores muestran que

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & -1 \\ 20 & 23 & -21 \end{pmatrix}\begin{pmatrix} 2 & 3 & 2 \\ 1 & 6 & 4 \\ 3 & -2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 14 & -32 \\ 0 & 1 & -2 \\ 0 & -5 & 11 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 48 \end{pmatrix}$$

## 5.10. Teorema de estructura de los grupos abelianos finitamente generados

**Teorema 5.10.1.** *Sea $G$ un subgrupo no nulo de $\mathbb{Z}^n$, con $n$ un entero positivo. Entonces existe una base $\{b_1, \dots, b_n\}$ de $\mathbb{Z}^n$ y una base $\{a_1, \dots, a_t\}$ (con $t \leq n$) de $G$ tal que $a_i = d_i b_i$, $i \in \{1, \dots, t\}$, con $d_i$ enteros positivos de forma que $d_i | d_{i+1}$ para todo $i \in \{1, \dots, n-1\}$. Por tanto*

$$\mathbb{Z}^n / G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_t} \times \mathbb{Z}^{n-t}.$$

*Demostración.* Sabemos que $G$ es un grupo libre por ser un subgrupo de $\mathbb{Z}^n$. Sea $\{g_1, \dots, g_t\}$ una base de $G$. Para cada $i \in \{1, \dots, t\}$, $g_i = (g_{1_i}, \dots, g_{n_i}) \in \mathbb{Z}^n$. Por tanto la matriz $A = (g_{i_j})$ es la matriz de la inclusión $i : G \to \mathbb{Z}^n$ respecto de las bases $\{g_1, \dots, g_t\}$ en $G$ y $\{e_1, \dots, e_n\}$ en $\mathbb{Z}^n$. Por lo visto en la sección anterior, podemos encontrar matrices $P$ y $Q$ de forma que

$$PAQ = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & d_t \\ 0 & \dots & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix},$$

con $d_i | d_{i+1}$. Las matrices $P$ y $Q$ se pueden ver como matrices de cambio de base. Respecto de estas nuevas bases $a_k = i(a_k) = d_k b_k$ para $k \in \{1, \dots, t\}$.

Como las columnas de $A$ forman una base de $G$, también lo hacen las de $AQ$. Además, la igualdad $AQ = P^{-1}D$, nos dice que la base en $\mathbb{Z}^n$ que buscamos son las columnas de $P^{-1}$. □

**Teorema 5.10.2** (Teorema de estructura)**.** *Sea $A$ un grupo abeliano finitamente generado. Entonces*

$$A \cong \mathbb{Z}^n \times \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k},$$

*donde $d_i$ divide a $d_{i+1}$ para $i = 1, \dots, k-1$.*

*Los números $n, d_1, \dots, d_t$ están determinados de manera única.*

*Demostración.* Supongamos que $A = \langle a_1, \dots, a_s \rangle$. Sabemos que existe un epimorfismo $f : \mathbb{Z}^s \to A$, determinado por $f(e_i) = a_i$. El núcleo de $f$, $\ker(f)$, es un subgrupo de $\mathbb{Z}^s$, y por el Teorema de Isomorfía, $A \cong \mathbb{Z}^s / \ker(f)$. Usando el teorema anterior obtenemos el resultado buscado. □

**Definición 5.10.3.** El número $n$ se llama *rango o número de Betti* del grupo $A$. Los números $d_1, \dots, d_t$ son los *factores invariantes* del grupo $A$.

*Ejemplo* 5.10.4. Sabemos que $U(8) = \{1, 3, 5, 7\}$ y por tanto es un grupo abeliano de orden 4. Para todo $x \in U(8)$ se tiene que $x^2 = 1$, luego todo elemento de $U(8)$ tiene orden dos. Salvo isomorfismos, los únicos grupos abelianos de orden 4 son

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \quad \text{y} \quad \mathbb{Z}_4.$$

Como $\mathbb{Z}_4$ tiene un elemento de orden 4, nos queda que $U(8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

*Ejemplo* 5.10.5. Calculemos todos los grupos abelianos finitos de orden 30. Claramente $\mathbb{Z}_{30}$ es uno de ellos. Supongamos que hubiese otro. Entonces sería de la forma $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k}$ con $d_1 | d_2 | \cdots | d_k$ y $d_1 \cdots d_k = 30$. Como $30 = 2 \cdot 3 \cdot 5$, no se puede encontrar una cadena de la forma anterior (salvo $d_1 = 30$).

*Ejemplo* 5.10.6. Veamos ahora cuántos grupos abelianos finitos hay de orden 12. Como $12 = 2^2 \cdot 3$,

- $d_1 = 12$, y
- $d_1 = 2, d_2 = 2 \cdot 3$,

son las únicas posibles secuencias $d_1, \ldots, d_k$ con $d_1|d_2|\cdots|d_k$ y $d_1 \cdots d_k = 12$. De esta forma sólo existen (salvo isomorfismo) dos grupos abelianos finitos de orden 12, $\mathbb{Z}_{12}$ y $\mathbb{Z}_2 \times \mathbb{Z}_6$.

Cuando $n$ es grande, puede resultar tedioso calcular todas las posibles secuencias $d_1, \ldots, d_k$ tales que $d_1|d_2|\cdots|d_k$ y $d_1 \cdots d_k = n$. Existe una forma más eficiente de resolver este problema, y la vamos a ver en la siguiente sección.

## 5.11. Grupos de torsión

Sea $A$ un grupo abeliano. Un elemento $a \in A$ se llama *de torsión* si existe un entero positivo $n$ tal que $na = 0$.

**Proposición 5.11.1.** *Sea $A$ un grupo abeliano arbitrario. El subconjunto de elementos de torsión*

$$\mathrm{Tor}(A) = \{a \in A \mid \exists n \in \mathbb{Z},\ n > 0\ na = 0\}$$

*es un subgrupo de $A$.*

Un grupo abeliano $A$ se llama *grupo de torsión* si todos sus elementos son de torsión.
Un grupo abeliano $A$ se llama *libre de torsión* si su único elemento de torsión es el neutro.

*Ejemplo* 5.11.2. Todo grupo finito es de torsión.

*Ejemplo* 5.11.3. Todo grupo abeliano libre es libre de torsión.

**Proposición 5.11.4.** *Sea $A$ un grupo abeliano arbitrario. El grupo cociente $A/\mathrm{Tor}(A)$ es libre de torsión.*

**Proposición 5.11.5.** *Un grupo abeliano finitamente generado es de torsión si y sólo si es finito.*

Naturalmente la definición de grupo abeliano libre puede extenderse al caso de rango infinito y todo grupo abeliano es isomorfo a un cociente de un grupo abeliano libre. Pero a nosotros nos interesan principalmente los grupos abelianos finitamente generados. En este caso existe una caracterización muy sencilla.

**Proposición 5.11.6.** *Un grupo abeliano finitamente generado es libre si y sólo si es libre de torsión.*

*Demostración.* Sea $A$ un grupo abeliano generado por $\{a_1, \ldots, a_n\}$. Ya sabemos que si $A$ es libre, entonces es libre de torsión. Para probar el recíproco, usamos el Teorema de estructura de grupos abelianos finitamente generados. □

Como consecuencia de esta caracterización obtenemos el siguiente resultado.

**Teorema 5.11.7.** *Todo grupo abeliano finitamente generado es isomorfo a la suma directa de un grupo abeliano libre y un grupo abeliano de torsión.*

*Demostración.* Sea $A$ un grupo abeliano finitamente generado. Consideramos la secuencia exacta corta

$$0 \to \mathrm{Tor}(A) \xrightarrow{i} A \xrightarrow{\pi} \frac{A}{\mathrm{Tor}(A)} \to 0.$$

Por la proposición anterior, $A/\mathrm{Tor}(A)$ es libre, lo que hace que dicha sucesión escinda, y en consecuencia $A \cong (A/\mathrm{Tor}(A)) \times \mathrm{Tor}(A)$. □

La demostración del teorema anterior también es consecuencia inmediata del teorema de estructura. Si

$$A \cong \mathbb{Z}^n \times \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k},$$

entonces $\mathbb{Z}^n$ es libre y por tanto libre de torsión, y $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k}$ es finito y por tanto de torsión. En este caso $\mathrm{Tor}(A) \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k}$.

Sabemos que la parte de torsión de un grupo abeliano finitamente generado es un grupo finito. Centrémonos por un momento en este tipo de grupos y veamos cómo se puede encontrar una descomposición alternativa a la del teorema de estructura.

Sea $A$ un grupo abeliano finito. Por el teorema de estructura de grupos abelianos finitamente generados, existen $d_1, \ldots, d_t$ enteros positivos con $d_i | d_{i+1}$ tales que

$$A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_t}.$$

Dado $d$ entero positivo, existen $p_1, \ldots, p_k$ primos distintos y $e_1, \ldots, e_k$ naturales tales que $d = p_1^{e_1} \ldots p_k^{e_k}$. Por el teorema chino del resto tenemos que

$$\mathbb{Z}_d \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

Si para cada $d_i$ de la descomposición de $A$ hacemos lo mismo, y luego agrupamos los primos convenientemente, obtenemos el siguiente resultado. Como $d_i | d_{i+1}$, los primos que aparecen son los de la factorización en primos de $d_t$. Es fácil comprobar que éstos son precisamente los que dividen a $|A|$.

**Teorema 5.11.8** (Descomposición cíclica primaria)**.** *Sea $A$ un grupo abeliano finitamente generado. Entonces*

$$A \cong \mathbb{Z}^n \times \mathbb{Z}_{p_1^{e_{11}}} \times \cdots \times \mathbb{Z}_{p_t^{e_{tk}}}$$

*y los números $n, p_1^{e_{11}}, \ldots, p_t^{e_{tk}}$ están determinados de manera única.*

**Definición 5.11.9.** Los números $p_1^{e_{11}}, \ldots, p_t^{e_{tk}}$ se llaman *divisores elementales* del grupo $A$.

**Definición 5.11.10.** Sea $p$ un primo. Un grupo $G$ (no necesariamente abeliano) se llama *p-primario* (o sencillamente *p-grupo*) si todo elemento $x \in G$ es de orden finito $p^k$ para algún $k$.

Sea $A$ un grupo abeliano y $p$ un primo. El siguiente resultado es fácil de probar.

**Proposición 5.11.11.** *El conjunto*

$$A_p = \{a \in A \mid p^k a = 0,\ k \geq 0\}$$

*es un subgrupo de $A$.*

**Definición 5.11.12.** El anterior subgrupo $A_p$ se llama *componente p-primaria de $A$*.

De lo dicho anteriormente, si $A$ es finito y $p$ es primo, entonces

$$A_p \cong \mathbb{Z}_{p^{f_1}} \times \cdots \times \mathbb{Z}_{p^{f_t}},$$

con $p^{f_i}$ el factor de $p$ en $d_i$ (de esta forma $f_1 \leq f_2 \leq \cdots \leq f_t$). De esta forma es fácil deducir los dos siguientes resultados.

**Proposición 5.11.13.** *Sea $A$ un grupo abeliano finito. Entonces $A_p \neq 0$ si y sólo si $p$ divide al orden $|A|$.*

**Teorema 5.11.14.** *Sea $A$ un grupo abeliano finito. Entonces $A$ se expresa de manera única como suma directa de p-grupos para primos diferentes $p$. Con mayor precisión, si $p_1, \ldots, p_t$ son los primos que dividen al orden $|A|$, entonces*

$$A = A_{p_1} \times \cdots \times A_{p_t}.$$

*Ejemplo* 5.11.15. Supongamos que queremos calcular todos los grupos abelianos (salvo isomorfismo) de orden $360 = 2^3 \cdot 3^2 \cdot 5$. Si $G$ es un grupo abeliano de orden 360, entonces $G \cong G_2 \times G_3 \times G_5$. Por tanto tenemos que ver cuántos 2-grupos hay de orden $2^3$, cuántos 3-grupos de orden $3^2$, y cuántos 5-grupos de orden 5. El único 5-grupo de orden 5 es $\mathbb{Z}_5$, así que basta con centrarnos en $G_2$ y $G_3$.

- Posibles $G_2$. Buscamos una secuencia $e_1 \leq \cdots \leq e_k$ tal que $e_1 + \cdots + e_k = 3$. Por tanto tendríamos $\{1,1,1\}$, $\{1,2\}$ y $\{3\}$. De esta forma los posibles $G_2$ son

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_8.$$

- Posibles $G_3$. Buscamos una secuencia $e_1 \leq \cdots \leq e_k$ tal que $e_1 + \cdots + e_k = 2$. Por tanto tendríamos $\{1,1\}$ y $\{2\}$. De esta forma los posibles $G_3$ son

$$\mathbb{Z}_3 \times \mathbb{Z}_3, \quad \mathbb{Z}_9.$$

De esta forma, todos los subgrupos de orden 360 son

$$\begin{array}{cc} \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}, & \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{180}, \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{90}, & \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_{120}, \\ \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_6 \times \mathbb{Z}_{60}, & \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_{360}. \end{array}$$

## 5.12. Presentaciones de grupos

Sea ahora $M$ un grupo abeliano finitamente generado por los elementos $u_1, \ldots, u_n$. y sea $F_2 \cong \mathbb{Z}^n$ un grupo abeliano libre con base $\mathcal{B}_2 = \{e_1, \ldots, e_n\}$ Por la propiedad universal del grupo abeliano libre y su corolario 5.5.6, existe un epimorfismo

$$\pi : F_2 \to M$$

definido por $\pi(e_i) = u_i$, $i = 1, \ldots, n$. Por el lema anterior el núcleo de $\pi$ es un subgrupo (abeliano libre) de $F_2$ finitamente generado por $m$ elementos $b_1, \ldots, b_m$ donde $b_j = a_{1j}e_1 + \cdots + a_{nj}e_n$, $j = 1, \ldots, m$. Sea $F_1$ un grupo abeliano libre de rango $m$ con base $\mathcal{B}_1 = \{f_1, \ldots, f_m\}$ y sea $\varphi : F_1 \to F_2$ el homomorfismo definido por $\varphi(f_j) = b_j$. La imagen de $\varphi$ es el grupo $K = \ker(\pi)$ y por el primer teorema de isomorfía,

$$M \cong \frac{F_2}{K} = \frac{F_2}{\mathrm{Im}(\varphi)}$$

Los elementos $b_j$ se aplican en cero, es decir que se verifica

$$a_{1j}u_1 + \cdots + a_{nj}u_n = 0 \qquad \text{para } j = 1, \ldots, m \tag{5.12.1}$$

**Definición 5.12.1.** Las ecuaciones 5.12.1 se llaman *relaciones* del grupo $M$.

Una *presentación* del grupo $M$ es la expresión

$$M = \langle u_1, \ldots, u_n \mid a_{1j}u_1 + \cdots + a_{nj}u_n = 0,\ j = 1, \ldots, m \rangle$$

El grupo abeliano $M$ está determinado salvo isomorfismos por la presentación, es decir, por el homomorfismo $\varphi$. Pero la presentación no es única: Depende de los generadores que elijamos para $M$ y $K$. Vamos a obtener otra presentación mas sencilla: Por el teorema 5.9.10 podemos cambiar la base de $F_1$ (es decir, cambiar los generadores de $\ker(\varphi)$ y la base de $F_2$ (es decir, cambiar los generadores de $F_2$ y de

$M$), de manera que respecto a las nuevas bases $\mathcal{B}'_1 = \{f'_1, \ldots, f'_m\}$ y $\mathcal{B}'_2 = \{e'_1, \ldots, e'_n\}$ al homomorfismo $\varphi$ le corresponda la matriz

$$A' = PAQ = \begin{pmatrix} d_1 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d_r & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & \ldots & 0 \end{pmatrix}$$

con $d_i \mid d_{i+1}$. Llamando $u'_i = \varphi(e'_i)$ obtenemos una nueva presentación para $M$:

$$M = \langle u'_1, \ldots, u'_n \mid d_1 u'_1 = 0, \ldots, d_r u'_r = 0 \rangle$$

que muestra inmediatamente que la descomposición cíclica de $M$ es

$$M \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_r\mathbb{Z}} \oplus \mathbb{Z}^{n-r} \cong \mathbb{Z}_{d_s} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z}^{n-r}$$

donde en la última expresión se han eliminado los factores triviales (los que corresponden a $d_i = 1$). Obsérvese que los factores invariantes de $M$ son los elementos de la diagonal principal de $A'$ distintos de cero y uno, y que el rango (o número de Betti) del grupo $M$ es la diferencia $n - r$ (número de generadores menos el rango de la matriz $A$).

*Ejemplo* 5.12.2. Consideramos el grupo dado por la presentación

$$M = \langle u_1, u_2, u_3 \mid 2u_1 + u_2 + 3u_3 = 0,\ 3u_1 + 6u_2 - 2u_3 = 0,\ 2u_1 + 4u_2 + 4u_3 = 0 \rangle$$

Queremos calcular su descomposición cíclica, sus factores invariantes y su rango. La matriz de la función $\varphi$ es

$$\begin{pmatrix} 2 & 3 & 2 \\ 1 & 6 & 4 \\ 3 & -2 & 4 \end{pmatrix}$$

La diagonalización de esta matriz es el ejemplo 5.9.16. Remitiéndonos a ese ejemplo, el grupo $M$ tiene rango 0 y un único factor invariante, $d_1 = 48$. Su descomposición cíclica es $M \cong \mathbb{Z}_{48}$, es decir que $M$ es cíclico. La matriz de cambio de base en $F_2$ es

$$P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & -1 \\ 20 & 23 & -21 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 21 & -1 \\ 1 & 0 & 0 \\ 3 & 20 & -1 \end{pmatrix}$$

Para los dos primeros elementos $e'_1, e'_2$ (cuyas coordenadas son las dos primeras columnas) tenemos que $\varphi(e'_1) = 0 = \varphi(e'_2)$. Así que el grupo $M$ es cíclico de orden 48, generado por la imagen del último elemento de la base,

$$v = \varphi(e'_3) = -u_1 - u_2$$

## 5.13. Ejercicios

**Ejercicio 5.1.** Calcular la forma normal, los factores invariantes y los divisores elementales de las siguientes matrices

$$\begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 7 & 10 & 6 \end{pmatrix} \quad \begin{pmatrix} -22 & -48 & -267 \\ -4 & -4 & 31 \\ -4 & -24 & 105 \\ 4 & -6 & -6 \end{pmatrix} \quad \begin{pmatrix} 9 & 4 & 5 \\ -4 & 0 & -3 \\ -6 & -4 & -2 \end{pmatrix} \quad \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix}$$

**Ejercicio 5.2.** Calcular los ordenes de todos los elementos de los distintos grupos abelianos de orden 8, 12, 16 y 24.

**Ejercicio 5.3.** Para los siguientes grupos calcular sus descomposiciones cíclicas.

1. $G_1 = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ con operación dada por multiplicación módulo 65.
2. $G_2 = \{1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134\}$ con operación dada por multiplicación módulo 135.
3. $G_3 = \{1, 7, 17, 23, 49, 55, 65, 71\}$ con operación dada por multiplicación módulo 96.
4. $G_4 = \{1, 4, 11, 14, 16, 19, 26, 29, 31, 34, 41, 44\}$ con operación dada por multiplicación módulo 45.

**Ejercicio 5.4.** Sea $G$ el grupo de las simetrías de un rectángulo (no cuadrado). Probar que $G$ es un grupo abeliano. Calcular sus descomposiciones cíclica y cíclica primaria.

**Ejercicio 5.5.** Listar todos los grupos abelianos no isomorfos de orden 10, 16, 20, 30 , 40 , 108 y 360, dando sus factores invariantes, divisores elementales y descomposiciones cíclicas y cíclicas primarias.

**Ejercicio 5.6.** Calcular la torsión y el anulador minimal del grupo abeliano $\mathbb{Q}/\mathbb{Z}$

**Ejercicio 5.7.** Para los siguientes grupos abelianos calcular sus rangos y sus descomposiciones cíclicas y cíclicas primarias:

a) $G_1 =< a, b, c; \begin{array}{rl} 3a + 9b + 9c & = 0 \\ 9a - 3b + 9c & = 0 \end{array} >$ ; b) $G_2 =< a, b, c; \begin{array}{rl} 2a + 2b + 3c & = 0 \\ 5a + 2b - 3c & = 0 \end{array} >$

c) $G_3 =< a, b, c, d; \begin{array}{rl} a + 3b + 2c & = 0 \\ 5a + 17b + 12c & = 0 \\ 6a + 4c & = 0 \end{array} >$ ; d) $G_4 =< a, b, c; \begin{array}{rl} 12a + 4b + 6c & = 0 \\ -4a + 2b + 8c & = 0 \\ -2a + 16b + 34c & = 0 \end{array} >$

e) $G_5 = \mathbb{Z}_{24} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_{35}$

¿Son algunos de estos grupos isomorfos?

**Ejercicio 5.8.** Dados los grupos abelianos:

$$G =< a, b, c, d; \begin{array}{rl} a + 2c - d & = 0 \\ a + 5c + 5d & = 0 \\ 2a + 4c + 2d & = 0 \end{array} > \qquad \text{y} \qquad H = \mathbb{Z}^3/K,$$

donde $K$ es el subgrupo con generadores $\{(1, 2, 7), (1, 4, 7), (-1, 0, 2)\}$. Calcular:

1. El rango, los factores invariantes y los divisores elementales de cada uno de ellos.
2. Sus descomposiciones cíclicas y cíclicas primarias.

3. Las descomposiciones cíclica y cíclica primaria de $G \oplus H$.

**Ejercicio 5.9.** 1. Encuentra todos los grupos abelianos distintos, salvo isomorfismo, de orden 500. Da para cada uno de ellos sus descomposiciones cíclica y cíclica primaria.

2. Calcula las descomposiciones cíclica y cíclica primaria de

$$G = \left\langle a, b, c \;\middle|\; \begin{array}{c} 3a - 3b + 9c = 0 \\ 6a + 12b - 9c = 0 \\ 12b + 9c = 0 \end{array} \right\rangle.$$

¿Cuantos elementos tiene $G$? ¿Tiene algún elemento de orden seis?

**Ejercicio 5.10.** Dados los grupos abelianos

$$G = \left\langle a, b, c \mid \begin{array}{c} 2a - 6b + 18c = 0 \\ 6a + 6c = 0 \end{array} \right\rangle$$

y

$$H = \mathbb{Z}^3/\langle (1, -9, 3), (1, -7, 1), (1, -1, 1) \rangle.$$

1. Calcula sus rangos, descomposiciones cíclicas y cíclicas primarias.
2. ¿Son isomorfos? ¿Lo son sus subgrupos de torsión?
3. ¿Cuántos elementos de orden 6 tiene $H$? ¿Y $G$?
4. ¿Cuantos grupos hay, salvo isomorfismos, con los mismos elementos que $H$?

**Ejercicio 5.11.** 1. Calcula la descomposición cíclica y cíclica primaria de todos los grupos abelianos no isomorfos de orden 484.

2. Sea

$$G = \left\langle a, b, c \mid \begin{array}{c} 2a + b + 4c = 0 \\ 2a + 2b + 6c = 0 \end{array} \right\rangle$$

y $H = \mathbb{Z}^2/K$, con $K$ el subgrupo de $\mathbb{Z}^2$ generado por los pares $(2, 3)$ y $(6, 3)$. Razona, calculando las descomposiciones cíclica y cíclica primaria de ambos, que no son isomorfos.

**Ejercicio 5.12.** Sea $u = (a, b) \in \mathbb{Z}^2$. Demostrar que $u$ puede completarse a una base del $\mathbb{Z}$-módulo $\mathbb{Z}^2$ si y solo si $a$ y $b$ son primos relativos. Encontrar $v \in \mathbb{Z}^2$ tal que $\{v, (2, 5)\}$ sea una base de $\mathbb{Z}^2$.

**Ejercicio 5.13.** Demostrar que $\mathbb{Q}$ no es un $\mathbb{Z}$-módulo finitamente generado. ¿Es $\mathbb{Q}$ un $\mathbb{Z}$-módulo libre?.

**Ejercicio 5.14.** ¿Es libre el $\mathbb{Z}$-módulo cociente $\mathbb{Z}[x]/(x^2 - 1)$? ¿Es libre el $\mathbb{Q}[x]$-módulo $\mathbb{Q}[x]/(x^2 - 1)$?.

**Ejercicio 5.15.** Encontrar una base para el submódulo de $\mathbb{Z}^3$ generado por a=(1,0,-1), b=(2,-3,1), c=(0,3,1), d=(3,1,5).

**Ejercicio 5.16.** Encontrar una base para el submódulo de $\mathbb{Q}[x]^3$ generado por $a = (2x - 1, x, x^2 + 3), b = (x, x, x^2), c = (x + 1, 2x, 2x^2 - 3)$.

## 5.14. Grupos abelianos usando GAP

### 5.14.1. Grupos abelianos finitamente generados

Para crear un grupo libre en GAPcon un número determinado de generadores, usamos el comando `FreeGroup`. Así, `FreeGroup(n)` crea un grupo con `n` generadores, que son `f.1,...,f.n` y que GAPpinta en pantalla como `f1,...,fn`. Si queremos que en vez de `fi`, GAPimprima con otros nombres los generadores, podemos pasar como argumentos dichos nombres.

```
gap> f:=FreeGroup("a","b");
<free group on the generators [ a, b ]>
gap> a:=f.1;;
gap> b:=f.2;;
gap> IsAbelian(f);
false
```

Esto hace que `f` sea un grupo libre sobre {`a`,`b`} no conmutativo por tener al menos dos generadores. A partir de ahora podemos usar `a` como primer generador de `f` y `b` como segundo generador.

Si queremos definir un grupo abeliano generado por dos elementos, como por ejemplo $\mathbb{Z}_6 \times \mathbb{Z}_{12}$, podemos usar una de sus presentaciones

$$\{a,\ b \mid 6a = 0, 12b = 0\}$$

y hacer un cociente de `f` "modulo" los relatores. Como por defecto GAPtrabaja con grupos no abelianos, debemos usar notación multiplicativa. Además, tenemos que explicitar que `a` y `b` conmutan.

Con el comando `Elements` podemos imprimir los elementos del nuevo grupo creado (no se debe usar este comando con `f`, que es infinito).

```
gap> g:=f/[a*b*(b*a)^(-1),a^6,b^12];
<fp group on the generators [ a, b ]>
gap> u:=g.1;;
gap> v:=g.2;;
gap> Elements(g);
[ <identity ...>, a^3, b^9, a^2, b^4, b^6, a^3*b^9, a^5, a^3*b^4, a^3*b^6,
  a^2*b^9, b, b^3, a^4, a^2*b^4, a^2*b^6, b^8, b^10, a^5*b^9, a^3*b, a^3*b^3,
  a, a^5*b^4, a^5*b^6, a^3*b^8, a^3*b^10, a^4*b^9, a^2*b, a^2*b^3, b^5, b^7,
  a^4*b^4, a^4*b^6, a^2*b^8, a^2*b^10, b^2, a*b^9, a^5*b, a^5*b^3, a^3*b^5,
  a^3*b^7, a*b^4, a*b^6, a^5*b^8, a^5*b^10, a^3*b^2, a^4*b, a^4*b^3, a^2*b^5,
  a^2*b^7, b^11, a^4*b^8, a^4*b^10, a^2*b^2, a*b, a*b^3, a^5*b^5, a^5*b^7,
  a^3*b^11, a*b^8, a*b^10, a^5*b^2, a^4*b^5, a^4*b^7, a^2*b^11, a^4*b^2,
  a*b^5, a*b^7, a^5*b^11, a*b^2, a^4*b^11, a*b^11 ]
gap> a*b=b*a;
false
gap> u*v=v*u;
true
gap> a in g;
false
gap> u in g;
true
```

Si queremos ver los generadores de un grupo, podemos usar el comando `GeneratorsOfGroup`, para ver los relatores, usamos `RelatorsOfFpGroup`. Aunque para eso el argumento tiene que ser un grupo del cual GAPsepa que es finitamente presentado. Lo cual queda claro para `g` por haber sido definido mediante una presentación finita.

```
gap> GeneratorsOfGroup(g);
[ a, b ]
gap> RelatorsOfFpGroup(g);
[ a*b*a^-1*b^-1, a^6, b^12 ]
```

Una forma alternativa y fácil de crear grupos finitos es a través del comando `CyclicGroup`, que crea un grupo cíclico del orden del argumento que le pasemos, combinarlo con el comando `DirectProduct` que a partir de dos o más grupos crea su producto directo. El problema es que gap no entiende la salida de `CyclicGroup` como un grupo finitamente presentado. Para arreglar ese pequeño problema, se puede usar el siguiente truco.

```
gap> g:=CyclicGroup(12);
<pc group of size 12 with 3 generators>
gap> IsCyclic(g);
true
gap> IsomorphismFpGroup(g);
[ f1, f2, f3 ] -> [ F1, F2, F3 ]
gap> Image(IsomorphismFpGroup(g));
<fp group of size 12 on the generators [ F1, F2, F3 ]>
gap> IsomorphismFpGroup(g);
[ f1, f2, f3 ] -> [ F1, F2, F3 ]
gap> gfp:=Image(last);
<fp group of size 12 on the generators [ F1, F2, F3 ]>
gap> RelatorsOfFpGroup(gfp);
[ F1^2*F2^-1, F2^-1*F1^-1*F2*F1, F3^-1*F1^-1*F3*F1, F2^2*F3^-1,
  F3^-1*F2^-1*F3*F2, F3^3 ]
gap> gs:=SimplifiedFpGroup(gfp);
<fp group on the generators [ F1 ]>
gap> RelatorsOfFpGroup(gs);
[ F1^12 ]
```

Como se ve, esta última salida es más “natural” que la inicial.

```
gap> d:=DirectProduct(CyclicGroup(4),CyclicGroup(15));
<pc group of size 60 with 4 generators>
gap> dfp:=SimplifiedFpGroup(Image(IsomorphismFpGroup(d)));
<fp group on the generators [ F1, F3 ]>
gap> RelatorsOfFpGroup(dfp);
[ F1^4, F3^-1*F1^-1*F3*F1, F3^15 ]
```

Un subgrupo finitamente generado de un grupo finitamente generado se puede definir usando el comando `Subgroup`.

```
gap> f:=FreeGroup("a","b");
<free group on the generators [ a, b ]>
gap> a:=f.1;
```

```
a
gap> b:=f.2;
b
gap> g:=f/[a*b*(b*a)^(-1),a^6,b^12];
<fp group on the generators [ a, b ]>
gap> h:=Subgroup(g,[g.1*g.2,g.2^2]);
Group([ a*b, b^2 ])
gap> IsAbelian(h);
true
```

El cociente de g por h se calcula usando simplemente /.

```
gap> IsCyclic(g/h);
```

El orden de un grupo se puede calcular con el comando `Order`, y el mínimo $m$ entero tal que $mx = 0$ para todo $x$ en el grupo (éste es el factor invariante más grande del grupo, también conocido como anulador minimal) con `Exponent`.

```
gap> Order(DirectProduct(CyclicGroup(3),CyclicGroup(10)));
30
gap> Exponent(DirectProduct(CyclicGroup(3),CyclicGroup(10)));
30
gap> Order(DirectProduct(CyclicGroup(3),CyclicGroup(15)));
45
gap> Exponent(DirectProduct(CyclicGroup(3),CyclicGroup(15)));
15
```

A continuación mostramos cómo definir una nueva función para calcular el orden de un elemento de un grupo.

```
#Orden de un elemento
 orden:=function(g,a)
 return Order(Subgroup(g,[a]));
 end;

gap> f:=FreeGroup("a","b");
<free group on the generators [ a, b ]>
gap> a:=f.1;; b:=f.2;;
gap> g:=f/[a*b*(b*a)^(-1),a^6,b^12];
<fp group on the generators [ a, b ]>
gap> u:=g.1;; v:=g.2;;
gap> orden(g,u);
6
gap> orden(g,v);
12
gap> orden(g,u*v);
12
gap> orden(g,u*v^2);
6

#Elementos de orden dado
```

```
elementosorden:=function(n,g)
return Filtered(Elements(g),a->orden(g,a)=n);
end;

gap> elementosorden(1,g);
[ <identity ...> ]
gap> elementosorden(2,g);
[ a^3, b^6, a^3*b^6 ]
gap> elementosorden(3,g);
[ a^2, b^4, a^4, a^2*b^4, b^8, a^4*b^4, a^2*b^8, a^4*b^8 ]
gap> elementosorden(g,6);
[ a^5, a^3*b^4, a^2*b^6, b^10, a, a^5*b^4, a^5*b^6, a^3*b^8, a^3*b^10,
  a^4*b^6, a^2*b^10, b^2, a*b^4, a*b^6, a^5*b^8, a^5*b^10, a^3*b^2, a^4*b^10,
  a^2*b^2, a*b^8, a*b^10, a^5*b^2, a^4*b^2, a*b^2 ]
gap> Length(last);
24
```

La función `AbelianInvariant` calcula los divisores elementales de un grupo abeliano, por lo que podemos utilizarla para determinar si dos grupos son isomorfos.

```
sonisomorfos:=function(g,h)
return AbelianInvariants(g)=AbelianInvariants(h);
end;

gap> d:=DirectProduct(CyclicGroup(4),CyclicGroup(15));
<pc group of size 60 with 4 generators>
gap> dd:=AbelianGroup([4,5]);
<pc group of size 20 with 2 generators>
gap> dd:=AbelianGroup([4,15]);
<pc group of size 60 with 2 generators>
gap> AbelianInvariants(d);
[ 3, 4, 5 ]
gap> AbelianInvariants(dd);
[ 3, 4, 5 ]
gap> sonisomorfos(d,dd);
true
```

El comando `IndependentGeneratorsOfAbelianGroup` da un generador para cada una de las componentes de la descomposición cíclica primaria.

```
gap> f:=FreeGroup("a","b");
<free group on the generators [ a, b ]>
gap> a:=f.1;
a
gap> b:=f.2;
b
gap> g:=f/[a*b*(b*a)^(-1),a^6,b^12];
<fp group on the generators [ a, b ]>
gap> h:=Subgroup(g,[g.1*g.2,g.2^2]);
Group([ a*b, b^2 ])
```

```
gap> AbelianInvariants(h);
[ 3, 3, 4 ]
gap> IndependentGeneratorsOfAbelianGroup(h);
[ a*b*a*b*a*b, a*b*a*b*a*b*a*b, b^4 ]
gap> AbelianInvariants(g/h);
[ 2 ]
gap> k:=f/[a*b*a^-1*b^-1,b^2];
<fp group on the generators [ a, b ]>
gap> AbelianInvariants(k);
[ 0, 2 ]
gap> IndependentGeneratorsOfAbelianGroup(k);
Error, no method found! For debugging hints type ?Recovery from NoMethodFound
Error, no 3rd choice method found for 'IndependentGeneratorsOfAbelianGroup' on\
 1 arguments called from
<compiled or corrupted call value>  called from
<function>( <arguments> ) called from read-eval-loop
Entering break read-eval-print loop ...
you can 'quit;' to quit to outer loop, or
you can 'return;' to continue
brk>
```

GAPtiene una base de datos con grupos de orden pequeño. Si queremos acceder a ella, podemos usar los comandos `SmallGroup` y `AllSmallGroups`.

```
gap> AllSmallGroups(360,IsAbelian);
[ <pc group of size 360 with 6 generators>,
  <pc group of size 360 with 6 generators>,
  <pc group of size 360 with 6 generators>,
  <pc group of size 360 with 6 generators>,
  <pc group of size 360 with 6 generators>,
  <pc group of size 360 with 6 generators> ]
gap> List(last,AbelianInvariants);
[ [ 5, 8, 9 ], [ 2, 4, 5, 9 ], [ 3, 3, 5, 8 ], [ 2, 2, 2, 5, 9 ],
  [ 2, 3, 3, 4, 5 ], [ 2, 2, 2, 3, 3, 5 ] ]
gap> AllSmallGroups(72,IsAbelian);
[ <pc group of size 72 with 5 generators>,
  <pc group of size 72 with 5 generators>,
  <pc group of size 72 with 5 generators>,
  <pc group of size 72 with 5 generators>,
  <pc group of size 72 with 5 generators>,
  <pc group of size 72 with 5 generators> ]
gap> List(last,AbelianInvariants);
[ [ 8, 9 ], [ 2, 4, 9 ], [ 3, 3, 8 ], [ 2, 2, 2, 9 ], [ 2, 3, 3, 4 ],
  [ 2, 2, 2, 3, 3 ] ]
```

### 5.14.2. Forma normal de Smith

En GAPlas listas se expresan separando sus elementos por comas dentro de un par de corchetes. Así `[1,2,3]` es una lista con tres elementos, el 1, el 2 y el 3. Las matrices se representan como una lista de

listas. Cada una de esas listas es una fila de la matriz. De esta forma la matriz

$$\begin{pmatrix} 9 & 4 & 5 \\ -4 & 0 & -3 \\ -6 & -4 & -3 \end{pmatrix}$$

se puede definir de la siguiente forma.

```
gap> m:=[[9,4,5],[-4,0,-3],[-6,-4,-3]];
[ [ 9, 4, 5 ], [ -4, 0, -3 ], [ -6, -4, -3 ] ]
```

Si queremos calcular su forma normal de Smith, usamos el comando `SmithNormalFormIntegerMat`.

```
gap> SmithNormalFormIntegerMat(m);
[ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 4 ] ]
```

Si lo que buscamos son las matrices de cambio de base, entonces usamos el comando `SmithNormalFirmIntegerMatTransforms`. Para acceder a un campo de un registro se usa la sintaxis `registro.campo`.

```
gap> fnsm:=SmithNormalFormIntegerMatTransforms(m);
rec( normal := [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 4 ] ],
  rowC := [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ],
  rowQ := [ [ 3, 2, 3 ], [ -4, -3, -4 ], [ -10, -9, -9 ] ],
  colC := [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 1, 1 ] ],
  colQ := [ [ 1, 0, 0 ], [ 0, 1, -1 ], [ 0, 0, 1 ] ], rank := 3, signdet := -1,
  rowtrans := [ [ 3, 2, 3 ], [ -4, -3, -4 ], [ -10, -9, -9 ] ],
  coltrans := [ [ 1, 0, 0 ], [ 0, 1, -1 ], [ 0, 1, 0 ] ] )
gap> fnsm.rowtrans*m*fnsm.coltrans;
[ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 4 ] ]
```

Si lo único que queremos son los factores invariantes, podemos usar lo siguiente.

```
gap> ElementaryDivisorsMat(m);
[ 1, 1, 4 ]
```

Para calcular los divisores elementales a partir de una lista de factores invariantes, usamos `AbelianInvariantsOfList` (nótese que los nombres están cambiados respecto a nuestras definiciones).

```
gap> AbelianInvariantsOfList(last);
[ 4 ]
gap> AbelianInvariantsOfList([6,12]);
[ 2, 3, 3, 4 ]
```

## 5.15. Grupos abelianos usando MATHEMATICA

Un grupo abeliano finitamente generado está determinado, de forma única salvo isomorfismo, por su rango (o número de Betti) y sus factores invariantes (o sus divisores elementales). En el caso finito el rango es cero y sólo hay que atender a éstos últimos. En MATHEMATICA podemos determinarlos utilizando un paquete externo para el cálculo de la forma normal de Smith, o alternativamente efectuando el cálculo de forma directa como veremos en la segunda parte de esta práctica.

### 5.15.1. Forma normal de Smith de una matriz con entradas enteras. Aplicación a grupos abelianos.

Utilizaremos el siguiente paquete

```
<<"c:/IntegerSmithNormalForm.m"
```

que nos permite calcular la forma normal de Smith de una matriz con coeficientes enteros. Sea la matriz

```
m ={ {1,4,10}, {2,36,4}, {0,24,4}, {16,30,6} }; MatrixForm[m]
```

$$\begin{pmatrix} 1 & 4 & 10 \\ 2 & 36 & 4 \\ 0 & 24 & 4 \\ 16 & 30 & 6 \end{pmatrix}$$

Calculamos:

```
m1 =SmithForm[m]; MatrixForm[m1]
```

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}$$

Podemos además determinar matrices $P$ y $Q$ tales que `P.m.Q = m1` con la función

```
ExtendedSmithForm[m]
```

```
{ { {1,0,0}, {0,2,0}, {0,0,4}, {0,0,0} },
{ { {1,0,0,0}, {16,0,-38,-1}, {46,201,-274,-28}, {-102,-445,607,62} },
  { {1,-10,-4394}, {0,0,1}, {0,1,439} } } }
```

Mejoremos la salida:

```
L  = ExtendedSmithForm[m]; MatrixForm[L[[1]]]
P  = L[[2,1]]; MatrixForm[P]
Q1 = L[[2,2]]; \text{MatrixForm}[Q1]
```

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 16 & 0 & -38 & -1 \\ 46 & 201 & -274 & -28 \\ -102 & -445 & 607 & 62 \end{pmatrix}$$

$$\begin{pmatrix} 1 & -10 & -4394 \\ 0 & 0 & 1 \\ 0 & 1 & 439 \end{pmatrix}$$

Comprobamos que efectivamente `P.m.Q1 = SmithForm[m]`:

```
MatrixForm[P.m.Q1]
```

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}$$

Este cálculo de la forma normal nos permite clasificar cualquier grupo abeliano dado en términos de generadores y relaciones. En efecto, sabemos que los factores invariantes del grupo abeliano son los factores invariantes de la matriz transpuesta de la de coeficientes de las relaciones. Por tanto, basta calcular la forma normal de dicha matriz. En cuanto al rango, sabemos que es la diferencia entre el número de generadores y el de relaciones (siempre supuestas independientes).

*Ejemplo* 5.15.1. Determinar las descomposiciones cíclica y cíclica primaria del grupo abeliano $G$ que tiene la siguiente presentación:

$$G = \langle x, y, z, t \mid 4x + 16y - 10z + 12t = 0,\ 20x - 30y + 16z - 24t = 0,\ 2x - 8z = 0 \rangle$$

Calculamos:

```
m = Transpose[ { {4,16,-10,12}, {20,-30,16,-24}, {2,0,-8,0} } ];
MatrixForm[m]
```

$$\begin{pmatrix} 4 & 20 & 2 \\ 16 & -30 & 0 \\ -10 & 16 & -8 \\ 12 & -24 & 0 \end{pmatrix}$$

```
m1 = SmithForm[m]; MatrixForm[m1]
```

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

Por tanto, los factores invariantes son 2, 2, 6 y los divisores elementales son 2, 2, 2, 3. La descomposición cíclica de $G$ es $\mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6$, mientras que la descomposición cíclica primaria de $G$ es $\mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$.

### 5.15.2. Cálculo de factores invariantes y divisores elementales de forma directa.

Sabemos que el máximo común divisor de los menores de orden i de una matriz es el mismo que el de cualquier matriz equivalente a ella. Por tanto, pensando en la forma normal, tenemos que el primer factor invariante es el máximo común divisor de los menores de orden 1 y, en general, el $i$-ésimo factor invariante es el cociente del máximo común divisor de los menores de orden $i$ por el de los menores de orden $i-1$. Este es el hecho fundamental que usamos para definir las siguientes funciones.

```
mcdmenores[a_]:=With[{n = Min[Dimensions}[a]]},
  Table[GCD@@Flatten[Minors[a,i]],{i,1,n}]]
factoresinvariantes[a_] := Module}[{men,n},
  men := mcdmenores[a];
  n := Length}[men];
  Join[First[men]}, Table[men[[i]]/men[[i-1]],{i,2,n}]]
]
```

*Ejemplo* 5.15.2. Consideramos la matriz

```
m1 = { {1,2,3}, {4,5,6} }; MatrixForm[m1]
```

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$

Calculamos sus factores invariantes con la función

```
factoresinvariantes[m1]
```

$$\{1, 3\}$$

y para la matriz

```
m2 = { {2,3,2}, {1,6,4}, {3,-2,4} }; MatrixForm[m2]
```

$$\begin{pmatrix} 2 & 3 & 2 \\ 1 & 6 & 4 \\ 3 & -2 & 4 \end{pmatrix}$$

obtenemos

```
factoresinvariantes}[m2]
```

$$\{1, 1, 48\}$$

En el ejercicio propuesto anteriormente tenemos que

```
m = Transpose}[{ {4,16,-10,12}, {20,-30,16,-24}, {2,0,-8,0} }]; MatrixForm[m]
```

$$\begin{pmatrix} 4 & 20 & 2 \\ 16 & -30 & 0 \\ -10 & 16 & -8 \\ 12 & -24 & 0 \end{pmatrix}$$

Sus factores invariantes son

```
factoresinvariantes[m]
```

$$\{2, 2, 6\}$$

Vamos ahora a calcular los divisores elementales. Para ello usamos la función `FactorInteger[n]`: que devuelve los primos en la factorización de $n$ con sus correspondientes exponentes. Por ejemplo

```
FactorInteger[15]
```

$$\{\{3,1\},\{5,1\}\}$$

A partir de la lista de factores invariantes, calculamos la de divisores elementales con la función

```
divisoreselementales[{}] := {};
divisoreselementales[{n_, ns___}] :=
  Join[FactorInteger[n], divisoreselementales[{ns}]]
```

Así obtenemos los divisores elementales del grupo del ejemplo anterior con el mandato

```
divisoreselementales[{2,2,6}]
```

$$\{\{2,1\},\{2,1\},\{2,1\},\{3,1\}\}$$

### 5.15.3. Cálculo de grupos abelianos de un orden dado

Pretendemos calcular todas las listas posibles de divisores elementales que puede tener un grupo de un orden dado. De esta forma clasificamos todos los grupos de un orden dado. Para ello, una vez factorizado el orden como producto de potencias de primos distintos, atenderemos a las particiones de cada uno de los exponentes y multiplicaremos entre si las distintas posibilidades. Definimos sucesivamente las siguientes funciones auxiliares hasta llegar a la función que proporcione las listas de los distintos grupos del orden dado.

Empezamos calculando todas las particiones $\{a_1,\ldots,a_k\}$ de un entero positivo $n$ de forma que $a_1+\cdots+a_k=n$ con $a_i\leq a_{i+1}$. Sea $\{a_1,\ldots,a_k\}$ una de esas particiones para $n$. Añadiendo un uno a cualquier $a_i$ que verifique que $a_i<a_{i+1}$, obtenemos una partición de numeros no decrecientes para $n+1$. Incrementando $a_k$ en uno, también obtenemos una partición para $n+1$. Obsérvese que $\{1,a_1,\ldots,a_k\}$ es también una partición de $n+1$. De esta forma , a partir de una o más particiones para $n$, podemos encontrar particiones para $n+1$. De esto se encarga la función `hijos` en conjunción con `agranda`.

```
agranda[ns_, i_, n_] :=
  ns + IdentityMatrix[n][[i]]/;i<n && ns[[i]]<ns[[i+1]]
agranda[ns_, n_, n_] := ns+IdentityMatrix[n][[n]]
agranda[_, _, _] := {}
```

```
agranda[{1,1,3}, 3, 3]
```

```
{1, 1, 4}
```

```
Table[agranda[{1, 2, 3}, i, 3], {i, 1, 3}]
```

```
{{2,2,3},{1,3,3},{1,2,4}}
```

```
hijos[{ns___}] := Select[With[{n=Length[{ns}]},
   Join[{{1, ns}}, Table[agranda[{ns}, i, n], {i, 1, n}]]
  ], # != {} &]
```

```
hijos}[{1, 1, 1}]
```

```
{{1,1,1,1},{1,1,2}}
```

Así para calcular las particiones de $n$, procedemos de forma recursiva calculando las de $n-1$ y aplicando los criterios anteriores. El caso base es para $n = 1$, que tiene una única partición, a saber $\{1\}$.

```
particion[1] := {{1}};
particion[n_Integer] :=
  Union[Flatten[Map[hijos, particion[n-1]], 1]]
```

```
particion[5]
```

```
{{5},{1,4},{2,3},{1,1,3},{1,2,2},{1,1,1,2},{1,1,1,1,1}}
```

Multiplicamos ahora entre sí todas las posibles soluciones encontradas, usando la función producto, que simplemente hace un producto cartesiano de dos listas, concatenando todas las listas del primer argumento a todas y cada una de las del segundo argumento.

```
producto[{}, _] := {}
producto[_, {}] := {}
producto}[{x_, xs___}, {y_, ys___}] :=
 Join[{Join[x,y]}, producto[{x},{ys}], producto[{xs}, {y}],
  producto[{xs}, {ys}}]]
```

```
producto[{{2, 2}, {3, 1}}, {{1, 1}, {4, 4}}]
```

```
{{2,2,1,1},{2,2,4,4},{3,1,1,1},{3,1,4,4}}
```

Utilizamos ahora las funciones que acabamos de implementar. Para ello factorizamos un entero usando el comando `FactorInteger`, que devuelve una lista de parejas cuyas primeras componentes son los primos que dividen al entero y su segunda componente indica el exponente con el que aparece en su factorización ese primo. A cada exponente le aplicamos la función partición, y luego con la función producto hacemos todos los posibles emparejamientos entre los distintos primos. De esto se encarga la función `usaparticion`, que es llamada desde `gruposdeorden`.

```
usaparticion[{}] := {}
usaparticion[{{p_, n_}}] := p^(particion[n])
usaparticion}[{{p_}, n_}, ps___}] :=
  producto[p^(particion[n]), usaparticion[{ps}]]
```

```
usaparticion[{{2, 2}, {3, 1}}]
```

```
{{4, 3}, {2, 2, 3}}
```

```
gruposdeorden[n_] := usaparticion[FactorInteger[n]]
```

```
gruposdeorden[12]
```

```
{{4, 3}, {2, 2, 3}}
```

Es decir, hay dos grupos no isomorfos de orden 12 que son $\mathbb{Z}_4 \oplus \mathbb{Z}_3$ y $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$.

```
gruposdeorden[360]
```

```
{{8, 9, 5}, {8, 3, 3, 5}, {2, 4, 9, 5},
{2, 2, 2, 9, 5}, {2, 4, 3, 3, 5}, {2, 2, 2, 3, 3, 5}}
```

Es decir, hay seis grupos no isomorfos de orden 12 que son

$$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5;$$
$$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5;$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5;$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5;$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5;$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

**Se propone como ejercicio final encontrar solución a los ejercicios propuestos en la Relación 4 que puedan ser resueltos utilizando las funciones definidas en esta Práctica.**

# Capítulo 6

# Módulos sobre dominios euclídeos

## 6.1. El anillo de endomorfismos de un grupo abeliano

**Proposición 6.1.1.** *Sean $M, N$ dos grupos abelianos (escritos aditivamente) y sea* $\mathrm{Hom}(M,N)$ *el conjunto de homomorfismos de grupos abelianos con dominio $M$ y codominio $N$. Definimos una suma en* $\mathrm{Hom}(M,N)$ *como*

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

*Entonces* $\mathrm{Hom}(M,N)$ *es un grupo abeliano para esta operación, con elemento neutro la aplicación constante cero y opuesto dada por $(-f)(x) = -f(x)$.*

**Proposición 6.1.2.** *Sea $M$ un grupo abeliano (escrito aditivamente) y sea* $\mathrm{End}(M)$ *el conjunto de endomorfismos de $M$. Definimos un producto como*

$$(f \cdot g)(x) = f(g(x))$$

*Entonces* $(\mathrm{End}(M), +, \cdot)$ *es un anillo, con unidad la aplicación identidad* $1 : M \to M$.

**Definición 6.1.3.** Llamamos *anillo de endomorfismos del grupo abeliano $M$* al anillo $\mathrm{End}(M)$ de la proposición 6.1.2

Llamamos *Anillo de endomorfismos* a cualquier subanillo de un anillo $\mathrm{End}(M)$.

*Ejemplo* 6.1.4. Tomando $M = (\mathbb{Z}, +)$, definimos una aplicación $\sigma : \mathrm{End}(M) \to \mathbb{Z}$ por $\sigma(f) = f(1)$. Esta aplicación es un isomorfismo de anillos.

*Ejemplo* 6.1.5. Sea $M = (\mathbb{Z}_n, +)$. Existe un isomorfismo de anillos $\sigma : \mathrm{End}(M) \cong \mathbb{Z}_n$ dado por $\sigma(f) = f(1)$.

*Ejemplo* 6.1.6. Sea $M = (\mathbb{Z} \times \mathbb{Z}, +)$. Para cada endomorfismo $f : M \to M$, sean $f(1,0) = (a,b)$ y $f(0,1) = (c,d)$. Definimos una aplicación

$$\sigma : \mathrm{End}(M) \to \mathcal{M}_2(\mathbb{Z}), \qquad \sigma(f) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

Es rutina comprobar que $\sigma$ es un isomorfismo de anillos.

Tenemos un teorema análogo al teorema de Cayley para grupos:

**Teorema 6.1.7.** *Cualquier anillo es isomorfo a un anillo de endomorfismos de un grupo abeliano.*

*Demostración.* La idea de la demostración es idéntica con la del teorema de Cayley (que se verá en la asignatura *Estructuras algebraicas*): Dado el anillo $(R, +, \cdot)$, consideramos el grupo aditivo $M = (R, +)$. Para cada $a \in R$ definimos la aplicación $a_I : M \to M$ por $a_I(x) = ax$ (que se llama *multiplicación por la izquierda definida por a*. Es inmediato comprobar las siguientes propiedades:

$$\begin{aligned} a_I(x+y) &= a_I(x) + a_I(y) \\ (a+b)_I(x) &= (a_I + b_I)(x) \\ (ab)_I(x) &= a_I(b_I(x)) \\ 1_I(x) &= x \end{aligned}$$

luego $a_I$ es un homomorfismo de grupos y la aplicación $\sigma : R \to \mathrm{End}(M)$ dada por $\sigma(a) = a_I$ es un homomorfismo de anillos. Siempre que sea $a_I = b_I$ tenemos que $a = a_I(1) = b_I(1) = b$, luego la aplicación $\sigma$ es inyectiva y tenemos un isomorfismo $R \cong \mathrm{Im}(\sigma) = R_I$ que es un subanillo de $\mathrm{End}(M)$. □

También es interesante considerar las multiplicaciones por la derecha: Con las notaciones de la demostración anterior para cada $a \in R$ definimos $a_D : M \to M$ como $a_D(x) = xa$. También es fácil comprobar las siguientes propiedades:

$$\begin{aligned} a_D(x+y) &= a_D(x) + a_D(y) \\ (a+b)_D(x) &= (a_D + b_D)(x) \\ (ab)_D(x) &= b_D(a_D(x)) \\ 1_D(x) &= x \end{aligned}$$

que nos dicen que la aplicación $a \mapsto a_D$ es un *antiisomorfismo de anillos* $R \to R_D$ (invierte el orden de multiplicación).

## 6.2. Definiciones y ejemplos

**Definición 6.2.1.** Sea $R$ un anillo. Un *módulo por la izquierda sobre R* o *R-módulo* $(M, +, \cdot)$ es un conjunto $M$ junto con una ley de composición interna $M \times M \to M$ dada por $(x, y) \mapsto x + y$ y una ley de composición externa $R \times M \to M$ denotada $(a, x) \mapsto ax$ que verifican los axiomas:

- *Asociatividad:* $\forall\, x, y, z \in M,\ x + (y + z) = (x + y) + z$
- *Existencia de cero:* $\exists\, 0 \in M,\ \forall\, x \in M,\ 0 + x = x = x + 0$
- *Existencia de opuesto:* $\forall\, x \in M,\ \exists\ -x \in M,\ x + (-x) = 0 = (-x) + x$
- *Conmutatividad:* $\forall\, x, y \in M,\ x + y = y + x$.

  Estos cuatro primeros axiomas pueden resumirse en uno: $(M, +)$ *es un grupo abeliano*.
- *Distributividad respecto a escalares:* $\forall\, a, b \in R,\ \forall\, x \in M,\ (a + b)x = ax + bx$
- *Distributividad respecto a vectores:* $\forall\, a \in R,\ \forall\, x, y \in M,\ a(x + y) = ax + ay$
- *Pseudoasociatividad:* $\forall\, a, b \in R,\ \forall\, x \in M,\ a(bx) = (ab)x$
- *Acción trivial del uno:* $\forall\, x \in M,\ 1 \cdot x = x$

Los elementos de $M$ se llaman *vectores* y los elementos de $R$ se llaman *escalares*.
En el caso particular en que $R$ es un cuerpo, $M$ se llama *espacio vectorial por la izquierda sobre* $R$.
De manera análoga se define el concepto de *módulo por la derecha sobre* $R$:

**Definición 6.2.2.** Sea $R$ un anillo. Un *módulo por la derecha sobre* $R$ $(M, +, \cdot)$ es un conjunto $M$ junto con una ley de composición interna $M \times M \to M$ dada por $(x, y) \mapsto x + y$ y una ley de composición externa $M \times R \to M$ denotada $(x, a) \mapsto xa$ que verifican los axiomas:

- *Asociatividad:* $\forall\ x, y, z \in M,\ x + (y + z) = (x + y) + z$
- *Existencia de cero:* $\exists\ 0 \in M,\ \forall\ x \in M,\ 0 + x = x = x + 0$
- *Existencia de opuesto:* $\forall\ x \in M,\ \exists\ -x \in M,\ x + (-x) = 0 = (-x) + x$
- *Conmutatividad:* $\forall\ x, y \in M,\ x + y = y + x$.
  Estos cuatro primeros axiomas pueden resumirse en uno: $(M, +)$ *es un grupo abeliano*.
- *Distributividad respecto a escalares:* $\forall\ a, b \in R\ \forall\ x \in M,\ x(a + b) = xa + xb$
- *Distributividad respecto a vectores:* $\forall\ a \in R,\ \forall\ x, y \in M,\ (x + y)a = xa + ya$
- *Pseudoasociatividad:* $\forall\ a, b \in R,\ \forall\ x \in M,\ (xa)b = x(ab)$
- *Acción trivial del uno:* $\forall\ x \in M,\ x \cdot 1 = x$

Los elementos de $M$ se llaman *vectores* y los elementos de $R$ se llaman *escalares*.
En el caso particular en que $R$ es un cuerpo, $M$ se llama *espacio vectorial por la derecha sobre* $R$.
Existe una definición alternativa de módulo por la izquierda: Para cada $R$-módulo por la izquierda $M$ y cada elemento $a \in R$ definimos una aplicación $a_I : M \to M$ como $a_I(x) = ax$.

**Proposición 6.2.3.** *1. La anterior aplicación $a_I$ es un endomorfismo de grupos abelianos.*

*2. La aplicación $\phi : R \to \mathrm{End}(M)$ dado por $\phi(a) = a_I$ es un homomorfismo de anillos*

Sea ahora $M$ un grupo abeliano y sea $R$ un anillo. Para cada homomorfismo $\psi : R \to \mathrm{End}(M)$ definimos una ley de composición externa $R \times M \to M$ como $a \cdot x = \psi(a)(x)$.

**Proposición 6.2.4.** *El grupo abeliano $M$ junto con la acción anterior es un $R$-módulo por la izquierda.*

**Proposición 6.2.5.** *Sean $M$ un grupo abeliano y $R$ un anillo. Existe una biyección entre las estructuras de $R$-módulos por la izquierda sobre $M$ y los homomorfismos $R \to \mathrm{End}(M)$.*

Construcciones duales a las anteriores producen el siguiente resultado:

**Proposición 6.2.6.** *Sean $M$ un grupo abeliano y $R$ un anillo. Existe una biyección entre las estructuras de $R$-módulos por la derecha sobre $M$ y los antihomomorfismos $R \to \mathrm{End}(M)$.*

*Ejemplo* 6.2.7. Todo grupo abeliano $M$ es un $\mathbb{Z}$-módulo: Para $m \in \mathbb{Z},\ m > 0$ se define inductivamente $mx = (m-1)x + x = x + \cdots + x$ ($m$ sumandos) y para $m < 0$ se define $mx = (-m)(-x) = (-x) + \cdots + (-x)$ (esta es la única acción posible de $\mathbb{Z}$ sobre $M$).

La observación de que los $\mathbb{Z}$-módulos son exactamente los grupos abelianos permite subsumir la teoría de grupos abelianos en la de módulos.

*Ejemplo* 6.2.8. Sea $R$ un anillo arbitrario y sea $M = (R, +)$ el grupo aditivo de $R$. El anillo $R$ actúa sobre $M$ mediante multiplicación por la izquierda: $ax$ es el producto interno definido en $R$. Así que $R$ es un $R$-módulo por la izquierda, que se conoce como *el $R$-módulo por la izquierda regular* . (Similarmente el anillo $R$ también es un $R$-módulo por la derecha, conocido como *el $R$-módulo por la derecha regular*).

*Ejemplo* 6.2.9. Sean $F$ un cuerpo, $V$ un espacio vectorial sobre $F$ y $t : V \to V$ una aplicación lineal. La aplicación $t$ verifica las condiciones:

$$\begin{aligned} \forall u, v \in V \quad & t(u+v) = t(u) + t(v) \\ \forall a \in F,\ \forall u \in V \quad & t(au) = at(u) \end{aligned}$$

La primera de estas condiciones dice que $t \in \mathrm{End}(V)$ y la segunda es que para toda multiplicación $a_I : V \to V$ se verifica que $ta_I = a_I t$. Por tanto el subanillo $F_I[t]$ de $\mathrm{End}(V)$ generado por $F_I = \{a_I \mid a \in F\}$ y $t$ es counmutativo. Por la propiedad universal del anillo de polinomios $F[X]$ existe un único homomorfismo de anillos $\Phi : F[X] \to \mathrm{End}(V)$ tal que $\Phi(X) = t$ y $\Phi(a) = a_I$ para todo $a \in F$.

El homomorfismo $\Phi$ dota a $V$ de una estructura de módulo por la izquierda sobre $F[X]$. Explícitamente,sea $p(X) = a_m X^m + \cdots + a_1 X + a_0$. Para cualquier vector $u \in V$ tenemos

$$p(X) \cdot u = a_m t^m(u) + \cdots + a_1 t(u) + a_0 u$$

De esta manera podemos derivar la teoría de una sola transformación lineal sobre un espacio vectorial de dimensión finita del estudio de este $F[X]$-módulo.

*Observación* 6.2.10. Sea $V = \mathbb{R}^n$. Sea $t : V \to V$ definida por $t(u) = t(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha_n, \alpha_1, \ldots, \alpha_{n-1})$. Determinar $Xu$, $(X^2 + 2)u$, $(X^{n-1} + X^{n-2} + \cdots + 1)u$. ¿Que vectores satisfacen $(X^2 - i)u = 0$?

## 6.3. Resultados básicos

**Lema 6.3.1** (Reglas de cálculo)**.** *Sea $R$ un anillo y sea $M$ un $R$-módulo arbitrario.*

1. *Para todo $a \in R$ se verifica*
$$a \cdot 0 = 0$$

2. *Para todo $a \in R$ y todo $u \in M$ se verifica*
$$a(-u) = -(au)$$

3. *Para todo $u \in M$ se verifica*
$$0 \cdot u = 0$$

4. *Para todo $a \in R$ y todo $u \in M$ se verifica*
$$(-a)u = -(au)$$

5. *Para todo $a \in R$ y cualesquiera $u_1, \ldots, u_m \in M$ se verifica*
$$a\left(\sum u_i\right) = \sum au_i$$

6. *Para cualesquiera $a_1 \ldots a_m \in R$ y todo $u \in M$ se verifica*
$$\left(\sum a_i\right) u = \sum a_i u$$

### 6.3.1. Homomorfismos

Sea $R$ un anillo y sean $M$ y $N$ dos $R$-módulos por la izquierda.

**Definición 6.3.2.** Un *homomorfismo de R-módulos* es una aplicación $f : M \to N$ que verifica:

$$\forall x, y \in M \; f(x+y) = f(x) + f(y)$$
$$\forall a \in R \; \forall x \in M \; f(ax) = af(x)$$

El módulo $M$ se llama *dominio* de $f$ y el módulo $N$ se llama *codominio* o *rango* de $f$.

El conjunto $\mathrm{Im}(f) = f(M) = \{f(x) \mid x \in M\} \subset N$ se llama *imagen de* $f$ y el conjunto $\ker(f) = \{x \in M \mid f(x) = 0\} \subset M$ se lama *núcleo de* $f$

El homomorfismo de módulos $f$ se llama *monomorfismo* si es una aplicación inyectiva, se llama *epimorfismo* si es una aplicación suprayectiva. Se llama *isomorfismo* si es una biyección y se representa por $f : M \cong N$.

Si el dominio y el codominio coinciden, $M = N$, diremos que $f$ es un *endomorfismo*. Un endomorfismo biyectivo se llama *automorfismo*.

**Proposición 6.3.3.** *1. Para todo módulo $M$ la aplicación identidad $1_M : M \to M$ es un automorfismo.*

2. *Sean $f_1 : M \to N$, $f_2 : N \to L$ dos homomorfismos de módulos. Entonces la aplicación compuesta $f_2 f_1 : M \to L$ es un homomorfismo.*

3. *Sea $f : M \to N$ un isomorfismo de módulos. Entonces la aplicación inversa $f^{-1} : N \to M$ también es un isomorfismo.*

4. *Sean $f_1, f_2 : M \to N$ y sea $a \in R$ arbitrario dos homomorfismos de módulos. Entonces las aplicaciones $f_1 + f_2, af_1 : M \to L$ son homomorfismos.*

**Corolario 6.3.4.** *Para dos módulos arbitrarios $M, N$ el conjunto de todos los homomorfismos $f : M \to N$ forman un $R$-módulo (con la suma y el producto por escalares como operaciones) que se representa por* $\mathrm{Hom}_R(M, N)$.

*Para un módulo arbitrario $M$, el conjunto de todos los endomorfismos de $M$ forman un anillo (con la suma y la composición de aplicaciones como operaciones), que se llama* anillo de los endomorfismos de $M$ *y se representa por* $\mathrm{End}_R(M)$

*Para un módulo arbitrario $M$, el conjunto de todos los automorfismos de $M$ forman un grupo (con la composición de aplicaciones como operación), que se llama* grupo de los automorfismos de $M$ *y se representa por* $\mathrm{Aut}_R(M)$

### 6.3.2. Submódulos

Sea $R$ un anillo fijo. Todos los módulos que vamos a considerar son módulos por la izquierda sobre $R$.

**Definición 6.3.5.** Dados dos módulos $(M, +)$ y $(N, +)$, decimos que $N$ *es un submódulo de* $M$, y lo representamos por $N < M$, cuando $N$ es un subconjunto de $M$ y la aplicación de inserción $N \to M$ es un homomorfismo de módulos.

*Ejemplo* 6.3.6. Todo módulo $M$ tiene dos submódulos: El módulo formado sólo por el elemento cero, que es el *submódulo trivial*, y el mismo $M$, que es el *submódulo total*. Ambos son los *submódulos impropios*. Cualquier otro submódulo es un *submódulo propio*.

Por abuso de lenguaje se suele identificar al submódulo $(N, +)$ con el subconjunto $N$, ya que la ley de composición está determinada por el módulo $N$.

**Proposición 6.3.7** (Caracterizaciones de submódulo)**.** *1. Sea $M$ un módulo y sea $\emptyset \neq N \subset M$. Entonces $N$ es un submódulo de $M$ si y sólo si se verifica:*

a) *Para todo par de elementos $x, y \in N$ también $x + y \in N$.*

b) *Para todo $a \in R$ y todo $x \in N$ también $ax \in N$.*

*2. Sea $M$ un módulo y sea $\emptyset \neq N \subset M$. Entonces $N$ es un submódulo de $M$ si y sólo si se verifica: Para todo par de escalares $a, b \in R$ y todo par de elementos $x, y \in N$ también $ax + by \in N$.*

*Ejemplo* 6.3.8. Para cualquier homomorfismo de módulos $f : M \to N$, el conjunto $\ker(f)$ es un submódulo de $M$ y el conjunto $\mathrm{Im}(f)$ es un submódulo de $N$.

*Ejemplo* 6.3.9. Sea $M$ un $\mathbb{Z}$-módulo. Para cualquier $N$ subgrupo de $M$, cualquier elemento $x \in N$ y cualquier entero positivo $n$ se verifica que $nx = x + \cdots + x \in N$. También $0x = 0 \in N$ y $(-n)x = -(nx) \in N$. Luego $N$ es un $Z$-submódulo de $M$. El inverso es inmediato, así que los $Z$-submódulos de $M$ son exactamente los subgrupos de $M$.

*Ejemplo* 6.3.10. Sea $V$ un espacio vectorial sobre un cuerpo $F$ y sea $t : V \to V$ un endomorfismo lineal. Sea $M = V$ el correspondiente $F[X]$-módulo. En este caso los $F[X]$-submódulos son sencillamente los $F$-subespacios vectoriales de $V$ que son *estables bajo* $t$, es decir los subespacios $W$ para los que $t(W) \subset W$.

*Ejemplo* 6.3.11. Sea $R$ un anillo considerado como $R$-módulo por la izquierda. Entonces los $R$-submódulos de $R$ son exactamente los ideales porla izquierda de $R$. De manera análoga, los $R$-submódulos de $R$ como $R$-módulo por la derecha son los ideales por la derecha.

**Proposición 6.3.12.** *Sea $L$ submódulo de $N$ y sea $N$ submódulo de $M$. Entonces $L$ es un submódulo de $M$.*

Como ilustración del criterio vamos a demostrar:

**Proposición 6.3.13.** *Sea $\{N_\lambda \mid \lambda \in \Lambda\}$ una familia de submódulos de un módulo $M$. Entonces $N = \cap_\lambda N_\lambda$ es un submódulo de $M$.*

Esta proposición nos permite definir dos conceptos importantes:

**Definición 6.3.14.** Sea $S$ un subconjunto de $M$. Llamamos *submódulo generado por* $S$ a la intersección $N$ de todos los submódulos de $M$ que contienen a $N$. Lo representamos por $N = R\langle S\rangle$.

**Proposición 6.3.15.** *Sean $N_1, N_2$ submódulos de $M$. Entonces $N_1 + N_2$ es un submódulo de $M$.*

**Proposición 6.3.16.** *1. Sea $S = \emptyset$. Entonces $\langle S\rangle$ es el submódulo trivial.*

*2. Para cualquier $S \subset M$ no vacío,*

$$R\langle S\rangle = \left\{ \sum a_x x \mid a_x \in R \text{ casi todos cero}, \ x \in S \right\}$$

*es el conjunto de todos los elementos de $G$ que se expresan como combinaciones lineales finitas de elementos de $S$ con coeficientes en $R$.*

### 6.3.3. Módulos cocientes

La construcción de modulos cocientes es similar a la de los grupos cocientes y los anillos cocientes. Si $N$ es un $R$-submódulo de un módulo $M$, consideramos el conjunto $M/N$ cuyos elementos son las clases $x + N = \{x + u \mid u \in N\}$. Definimos dos operaciones en $M/N$ como:

$$\forall x, y \in M, \quad (x + N) + (y + N) = (x + y) + N \tag{6.3.1}$$

$$\forall a \in R, \ \forall x \in M, \quad a(x + N) = ax + N \tag{6.3.2}$$

**Teorema 6.3.17.** *1. Las operaciones 6.3.1 están bien definidas (es decir, son independientes de los representantes $x$ elegidos.*

*2. El conjunto $M/N$ junto con las operaciones 6.3.1 es un $R$-módulo.*

*Ejemplo* 6.3.18. Se suele ver a la clase $x+N$ como el resultado de aplicar la "traslación" por $x$ al submódulo $N$. Mas concretamente, si $x$es un vector en un espacio vectorial real tridimensional y $N$ es un subespacio de dimensión dos, la clase $x + N$ es el conjunto de todos los vectores que están en el plano paralelo a $N$ que pasa por $x$.

Definimos una aplicación $p : M \to M/N$ como $p(x) = x + N$.

**Lema 6.3.19.** *La aplicación p es un homomorfismo de R-módulos, que se llama* proyección canónica *de M sobre M/N.*

## 6.3.4. Teoremas de isomorfismo

**Teorema 6.3.20.** *Cualquier homomorfismo de R-módulos $f : M \to M_1$ induce una biyección*

$$\{N \mid \ker(f) < N < M\} \cong \{N_1 \mid 1 < N_1 < \mathrm{Im}(f)\}$$

*que asigna a cada submódulo N que contenga a* $\ker(f)$ *su imagen $f(N)$, y cuya inversa asigna a cada submódulo $N_1$ contenido en* $\mathrm{Im}(f)$ *su imagen inversa $f^{-1}(N_1)$. Cada uno de estos conjuntos de submódulos es un retículo bajo el orden parcial dado por inclusión y esta biyección es un isomorfismo de retículos.*

**Teorema 6.3.21** (Teorema fundamental del módulo cociente)**.** *Sea N un submódulo de M. Para cada homomorfismo de módulos $f : M \to M_1$ con $f(N) = 0$ existe un único homomorfismo $f' : M/N \to M_1$ tal que $f = f'p$, siendo $p : M \to M/N$ la proyección canónica.*

La propiedad enunciada en el teorema 6.3.21 se conoce también como *propiedad universal del módulo cociente*.

**Corolario 6.3.22.** *En las condiciones del teorema 6.3.21,* $\mathrm{Im}(f') = \mathrm{Im}(f)$ *y* $\ker(f') = \ker(f)/N$.

**Corolario 6.3.23.** *Sea $f : M \to M_1$ es un epimorfismo de módulos con núcleo $N = \ker(f)$. Existe un isomorfismo único $f' : M/N \cong M_1$ tal que $f = f'p$.*

**Corolario 6.3.24.** *Sea $f : M \to M_1$ es un homomorfismo de módulos con núcleo N. Existe un monomorfismo único $f' : M/N \to M_1$ tal que $f = f'p$,* $\mathrm{Im}(f) = \mathrm{Im}(f')$.

**Corolario 6.3.25** (Descomposición canónica de un homomorfismo)**.** *Cualquier homomorfismo $f : M \to M_1$ con núcleo $N = \ker(f)$ e imagen $L = \mathrm{Im}(f)$ se escribe como un compuesto $i\sigma p$:*

$$M \xrightarrow{p} \frac{M}{N} \xrightarrow{\sigma} L \xrightarrow{i} M_1$$

*con p epimorfismo, $\sigma$ isomorfismo y la inclusión i monomorfismo.*

**Teorema 6.3.26** (Primer teorema de isomorfismo)**.** *Todo homomorfismo de módulos $f : M \to M_1$ induce un isomorfismo*

$$\sigma : \frac{M}{\ker(f)} \cong \mathrm{Im}(f)$$

*Demostración.* $\sigma$ es el isomorfismo dado en el corolario 6.3.25 anterior □

**Teorema 6.3.27.** *Sea $f : M \to M_1$ un homomorfismo de módulos con núcleo $N$ y sean $N', M'$ submódulos de $M$ con $N < N' < M' < M$. En este caso existe un isomorfismo*

$$\frac{M'}{N'} \cong \frac{f(M')}{f(N')} \qquad \text{dado por } x + N' \mapsto f(x) + f(N')$$

En particular para $N' = N$ obtenemos que $M'/N \cong f(M')$.

*Demostración.* Sea $N'$ submódulo de $M'$. Como el epimorfismo $f_1 : M' \to f(M')$ tiene núcleo $N$, es universal para este núcleo. O sea que la proyección $p : M' \to M'/N'$ factoriza como $p = p' f_1$ para un morfismo $p' : f(M') \to M'/N'$ y el núcleo de $p'$ es $f(N')$. Luego $M'/N' \cong f(M')/f(N')$, con $s + N' \mapsto f(s) + f(N')$ □

**Corolario 6.3.28** (Tercer teorema de isomorfismo)**.** *Dado un módulo $M$ y un submódulo suyo $N$, existe una biyección natural entre los submódulos de $M$ que contienen a $N$ y los submódulos de $M/N$ dada por $L \leftrightarrow L/N$. Además existe un isomorfismo*

$$\frac{M/N}{L/N} \cong \frac{M}{L}$$

*dado por $(m + N) + (L/N) \mapsto m + L$*

El tercer teorema de isomorfismo se llama también *teorema del doble cociente*

*Demostración.* Sea $f : M \to M/N$ la proyección canónica. La biyección buscada viene dada por el teorema 6.3.20: Cada submódulo de $M/N$ es de la forma $f(L)$ para algún $L$ con $N < L < M$. Pero la imagen $f(L)$ consiste en todas las clases $m + N$ con $m \in L$, luego $f(L) = L/N$. El teorema 6.3.27 con $S = M$ y $R = N$ nos da el resultado pedido. □

El teorema del doble cociente nos dice que que en un doble cociente podemos cancelar un denominador común.

**Teorema 6.3.29** (Segundo teorema de isomorfismo)**.** *Sea $M$ un módulo, sean $N$ y $L$ submódulos de $M$. Entonces existe un isomorfismo*

$$\frac{N}{N \cap L} \cong \frac{N + L}{L}$$

*dado por $m + (N \cap L) \mapsto m + L$.*

El segundo teorema de isomorfismo se conoce también como *teorema del paralelogramo*

*Demostración.* Sea $i : N \to N + L$ la inclusión y sea $p : N + L \to (N + L)/L$ la protección canónica. El compuesto $f = p \cdot i : N \to (N + L)/N$ es un homomorfismo de módulos. La imagen $\mathrm{Im}(f)$ del morfismo anterior es el módulo de las clases con elementos de $N$, luego es $(N + L)/L$. El núcleo consiste en el conjunto de elementos de $N$ que pertenecen a $L$, o sea $N \cap L$. Por el teorema 6.3.26, $N/(N \cap L) \cong (N + L)/L$ con $m + (N \cap L) \mapsto m + L$ □

### 6.3.5. Módulos cíclicos

**Definición 6.3.30.** Un $R$-módulo $M$ se llama *cíclico* si existe un $x_0 \in M$ tal que todo elemento de $M$ es de la forma $ax_0$ con $a \in R$. El elemento $x_0$ se llama *generador* de $M$.

**Definición 6.3.31.** Sea $M$ un $R$-módulo y sea $x \in M$.
Llamamos *anulador de* $x$ al conjunto

$$\mathrm{Ann}(x) = \{a \in R \mid ax = 0\}$$

Llamamos *anulador de* $M$ al conjunto

$$\mathrm{Ann}(M) = \{a \in R \mid \forall x \in M,\ ax = 0\}$$

Obsérvese que $\mathrm{Ann}(M) = \cap_{x \in M} \mathrm{Ann}(x)$

**Lema 6.3.32.** *Sea $M$ un $R$-módulo y sea $x \in M$. El conjunto* $\mathrm{Ann}(x)$ *es un ideal por la izquierda de $R$.*
*El conjunto* $\mathrm{Ann}(M)$ *es un ideal (bilátero) de $R$.*

**Lema 6.3.33.** *Todo módulo cíclico es isomorfo a un cociente del módulo regular por un ideal por la izquierda.*

*Demostración.* Sea $M = Rx_0$. Tenemos un homomorfismo $f : R \to M$ dado por $f(a) = ax_0$. El núcleo $\mathrm{Ann}(x_0) = \{a \in R \mid ax_0 = 0\}$ es el *anulador de $x_0$ en $R$*. La imagen es todo $M$. El primer teorema de isomorfismo dice que $M \cong R/\mathrm{Ann}(x_0)$ □

*Ejemplo* 6.3.34. En el caso en que $R = \mathbb{Z}$ tenemos que $\mathbb{Z}x \cong \mathbb{Z}$ o bien $\mathbb{Z}x = n\mathbb{Z}$ donde $n > 0$ es el menor entero positivo tal que $nx = 0$. Es decir que $n$ es el orden del elemento $x$ y del grupo cíclico $\langle x \rangle$. Así que para un elemento $x$ de un módulo $M$, podemos ver al ideal $\mathrm{Ann}(x)$ como una generalización del orden de un elemento de un grupo abeliano. Por esta razón en algunos libres se le llama *ideal orden* del elemento $x$.

### 6.3.6. $F[X]$-Módulos cíclicos

Sea $M$ un $F[X]$-módulo cíclico. Esto es decir que existe un vector $u \in M$ tal que $M = F[X]u = \{f \cdot u \mid f \in F[X]\}$. Como hemos visto en el ejemplo 6.2.9, el $F[X]$-módulo $M$ está determinado por un espacio vectorial $V$ (el mismo grupo aditivo que $M$, pero con los escalares restringidos a $F$) y un endomorfismo lineal $t : V \to V$ que corresponde a la multiplicación por $X$. Es decir que para todo vector $v \in V$ se tiene que $t(v) = X \cdot v$.

Sea $\mathrm{Ann}(u) = \{f \in F[X] \mid f \cdot u = 0\}$ el ideal orden de $u$. Existe un isomorfismo $F[X]/\mathrm{Ann}(u) \cong F[X]u = M$.

Si $\mathrm{Ann}(u) = 0$, esto nos dice que $M \cong F[X]$ es un espacio vectorial sobre $F$ de dimensión infinita, con base $\{u, X \cdot u, X^2 \cdot u, \dots\}$.

Si $\mathrm{Ann}(u) \neq 0$, existe un único polinomio mónico $g \in F[X]$ tal que $\mathrm{Ann}(u) = (g)$. Llamamos a este polinomio *$g$ el polinomio mínimo de $u$*. Sea explícitamente

$$g = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

Definimos sucesivamente los vectores

$$\begin{aligned} u_1 &= u, \\ u_2 &= X \cdot u = t(u), \\ &\dots \\ u_{i+1} &= X \cdot u_i = t(u_i) = X^i \cdot u = t^i(u), \\ &\dots \end{aligned}$$

**Proposición 6.3.35.** *El conjunto $\mathcal{B} = \{u_1, \dots, u_n\}$ es una base de $V$ sobre $F$.*

**Corolario 6.3.36.** *El espacio $V$ tiene dimensión $n = gr(p)$ sobre $F$.*

**Corolario 6.3.37.** *Respecto a la base $\mathcal{B}$, al endomorfismo $t$ le corresponde la matriz*

$$M(g) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$$

**Definición 6.3.38.** La anterior matriz $M(g)$ se llama *matriz asociada* al polinomio $g$.

*Ejemplo* 6.3.39. Sea $g = (X^2 + X + 1)^2 = X^4 + 2X^3 + 3X^2 + 2X + 1$. La correspondiente matriz asociada es

$$M(g) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & -3 \\ 0 & 0 & 1 & -2 \end{pmatrix}$$

*Ejemplo* 6.3.40. Un ejemplo muy parecido: Sea $g = (X^2 - 3X + 7)^2 = X^4 - 6X^3 + 23X^2 - 42X + 49$. La correspondiente matriz asociada es

$$M(g) = \begin{pmatrix} 0 & 0 & 0 & -49 \\ 1 & 0 & 0 & 42 \\ 0 & 1 & 0 & -23 \\ 0 & 0 & 1 & 6 \end{pmatrix}$$

*Ejemplo* 6.3.41. Sea ahora $g = (X - 2)^3 = X^3 - 6X^3 + 12X^2 - 8$. La matriz asociada de este polinomio es

$$M(g) = \begin{pmatrix} 0 & 0 & 8 \\ 1 & 0 & -12 \\ 0 & 1 & 6 \end{pmatrix}$$

En el caso particular en que $g = p^k$ con $p \in F[X]$ mónico e irreducible tenemos otra base interesante: Sea explícitamente

$$p = X^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$$

con $km = n$. Definimos ahora los vectores

$$\begin{aligned} v_1 &= u = u_1, \\ v_2 &= X \cdot u = u_2, \\ &\dots \\ v_m &= X^{m-1} \cdot u = u_m \\ v_{m+1} &= p \cdot u = X^m \cdot u + b_{m-1}v_m + \cdot + b_1v_2 + b_0v_1, \\ v_{m+2} &= X \cdot v_{m+1} = (Xp) \cdot u, \\ &\dots \\ v_{2m} &= X \cdot v_{2m-1} = (X^{m-1}p) \cdot u \\ v_{2m+1} &= p \cdot v_{m+1} = p^2 \cdot u \\ &\dots \end{aligned}$$

En general, $v_k = X^r v_{qm+1} = (X^r p^q) \cdot u$ donde $k - 1 = qm + r$ con $0 \leq r < m$.

**Proposición 6.3.42.** *El conjunto $\mathcal{B}_1 = \{v_1, \ldots, v_n\}$ es una base de $V$ sobre $F$.*

**Corolario 6.3.43.** *Respecto a la base $\mathcal{B}_1$, al endomorfismo $t$ le corresponde la matriz definida por bloques:*

$$J(p^k) = \begin{pmatrix} M(p) & 0 & 0 & \ldots & 0 & 0 \\ N & M(p) & 0 & \ldots & 0 & 0 \\ 0 & N & M(p) & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & M(p) & 0 \\ 0 & 0 & 0 & \ldots & N & M(p) \end{pmatrix}$$

*donde $M(p)$ es la matriz asociada a $p$ y $N = e_{1m}$ es la matriz cuadrada*

$$N = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

**Definición 6.3.44.** La anterior matriz $J(p^k)$ se llama *bloque de Jacobson* del polinomio $g$.

Un caso particular importante es cuando $p = X - a$ es un polinomio de grado $m = 1$ (Esto ocurre siempre cuando $F = \mathbb{C}$). Entonces la matriz $J(p)$ toma la forma

$$J(p) = J(a) = \begin{pmatrix} a & 0 & 0 & \ldots & 0 & 0 \\ 1 & a & 0 & \ldots & 0 & 0 \\ 0 & 1 & a & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & a & 0 \\ 0 & 0 & 0 & \ldots & 1 & a \end{pmatrix}$$

y se llama *bloque de Jordan* correspondiente al valor $a$.

*Ejemplo* 6.3.45. Sea $g = (X^2 + X + 1)^2 = X^4 + 2X^3 + 3X^2 + 2X + 1 \in \mathbb{Q}[X]$. El polinomio $p = X^2 + X + 1$ es irreducible y el bloque de Jacobson es

$$M(g) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

*Ejemplo* 6.3.46. Un ejemplo muy parecido: Sea $g = (X^2 - 3X + 7)^2 = X^4 - 6X^3 + 23X^2 - 42X + 49 \in \mathbb{Q}[X]$. El polinomio $p = X^2 - 3X + 7$ es irreducible y el bloque de Jacobson correspondiente es

$$M(g) = \begin{pmatrix} 0 & -7 & 0 & 0 \\ 1 & 3 & 0 & 0 \\ 0 & 1 & 0 & -7 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

*Ejemplo* 6.3.47. Sea ahora $g = (X - 2)^3 = X^3 - 6X^3 + 12X^2 - 8$. El bloque de Jordan de este polinomio es

$$M(g) = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

## 6.4. Sumas directas de módulos

Sea $R$ un anillo y sean $M_1, \ldots, M_n$ módulos por la izquierda sobre $R$. Sea $M = M_1 \times \cdots \times M_n$ el conjunto producto cartesiano de los $M_i$. Definimos en $M$ una suma y un producto externo por componentes:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n) \tag{6.4.1}$$

$$a(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n) \tag{6.4.2}$$

**Lema 6.4.1.** *El conjunto $M$ con las operaciones 6.4.1 es un módulo por la izquierda sobre $R$.*

**Definición 6.4.2.** El $R$-módulo $M$ se llama *suma directa (externa)*, *producto directo* o *biproducto* de los módulos $M_i$. Lo representamos como

$$M = M_1 \oplus \cdots \oplus M_n$$

Para este módulo definimos dos conjuntos de aplicaciones:
Para todo $i = 1, \ldots, n$ la $i$-ésima *proyección* es la aplicación

$$p_i : M \to M_i, \qquad p_i(x_1, \ldots, x_n) = x_i$$

y la $i$-ésima *inserción* es la aplicación

$$\lambda_i : M_i \to M, \qquad \lambda_i(x) = (0, \ldots, 0, x, 0 \ldots, 0)$$

(la $x$ en el lugar $i$).

**Lema 6.4.3.** *Para $i = 1, \ldots, n$ las aplicaciones $p_i$ y $\lambda_i$ son homomorfismos de $R$-módulos.*

**Proposición 6.4.4.** *Las proyecciones e inserciones tienen las siguientes propiedades:*

1. *Para todo $t = 1, \ldots, n$ se verifica $p_i\lambda_i = 1_{M_i}$ (la aplicación identidad en $M_i$).*
2. *Para todo par de índices $i \neq j$ se verifica $p_i\lambda_j = 0$.*
3. *Además se verifica que*
$$\lambda_1 p_1 + \cdots + \lambda_n p_n = 1_M$$
*(la aplicación identidad en $M$).*

**Teorema 6.4.5** (Propiedad universal del coproducto)**.** *Para toda familia de homomorfismos de $R$-módulos $f_i : M_i \to N$ existe un único homomorfismo de $R$-módulos $f : M \to N$ tal que para todo $i = 1, \ldots, n$ se verifica $f\lambda_i = f_i$*

Explícitamente, $f$ está definido por $f(x_1, \ldots, x_n) = f_1(x_1) + \cdots + f_n(x_n)$.

**Teorema 6.4.6** (Propiedad universal del producto)**.** *Para toda familia de homomorfismos de $R$-módulos $g_i : N \to M_i$ existe un único homomorfismo de $R$-módulos $f : N \to M$ tal que para todo $i = 1, \ldots, n$ se verifica $p_i g = g_i$*

Explícitamente, $g$ está definido por $g(y) = (g_1(y), \ldots, g_n(y))$.

**Proposición 6.4.7.** *Sean $M_1, \ldots, M_n$ módulos por la izquierda sobre $R$ y para cada índice $i$ sea $N_i$ un $R$-submódulo de $M_i$.*

1. *La suma directa $N = N_1 \oplus \cdots \oplus N_n$ es un $R$-submódulo de $M = M_1 \oplus \cdots \oplus M_n$.*

2. *Existe un isomorfismo de R-módulos*

$$\frac{M_1 \oplus \cdots \oplus M_n}{N_1 \oplus \cdots \oplus N_n} \cong \frac{M_1}{N_1} \oplus \cdots \oplus \frac{M_n}{N_n}$$

*dado explícitamente por*

$$(x_1, \ldots, x_n) + N \mapsto (x_1 + N_1, \ldots, x_n + N_n)$$

Sea ahora $M$ un módulo y sean $M_1, \ldots, M_n$ submódulos suyos. Por la propiedad universal del coproducto existe un homomorfismo

$$f : M_1 \oplus \cdots \oplus M_n \to M$$

definido por $f(x_1, \ldots, x_n) = x_1 + \cdots + x_n$

**Lema 6.4.8.** *La imagen del homomorfismo $f$ es el submódulo suma $M_1 + \cdots + M_n$.*

**Corolario 6.4.9.** *El homomorfismo $f$ es sobre si y sólo si $M = M_1 + \cdots + M_n$*

**Proposición 6.4.10.** *Las tres condiciones siguientes son equivalentes:*

1. *El homomorfismo $f$ es inyectivo*
2. *Para cada índice i se verifica $M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n) = 0$*
3. *Para cada índice i se verifica $M_i \cap (M_1 + \cdots + M_{i-1}) = 0$*

**Definición 6.4.11.** Cuando se verifican las condiciones de la proposición 6.4.10 decimos que los módulos $M_1, \ldots, M_n$ son *independientes*.

**Proposición 6.4.12.** 1. *Sean $M_1, \ldots, M_n$ submódulos independientes de M. Sean $N_1 = M_1 + \cdots + M_{r_1}$, $N_2 = M_{r_1+1} + \cdots + M_{r_1+r_2}$, $N_3 = M_{r_1+r_2+1} + \cdots + M_{r_1+r_2+r_3}$, etc. Entonces los submódulos $N1, N_2, N_3, \ldots$ son independientes.*

2. *Sean $M_1, \ldots, M_n$ submódulos independientes de M y supongamos que para $i = 1, \ldots, n$ tenemos que $M_i = M_{i1} \oplus M_{i2} \oplus \cdots \oplus M_{in_i}$ donde los $M_{ij}$ son submódulos de $M_i$. Entonces los submódulos*

$$M_{11}, \ldots, M_{1r_1}, M_{21}, \ldots, M_{2r_2}, \ldots, M_{n1}, \ldots, M_{nr_n}$$

*son independientes.*

**Definición 6.4.13.** El módulo $M$ se llama *suma directa interna* de los submódulos $M_1, \ldots, M_n$ si el homomorfismo $f$ es un isomorfismo.

Cuando $M$ es la suma directa interna de los submódulos $M_i$ denotamos directamente $M = M_1 \oplus \cdots \oplus M_n = \bigoplus_{i=1}^{n} M_i$

**Teorema 6.4.14** (Caracterizaciones de suma directa interna)**.** *Las tres condiciones siguientes son equivalentes:*

1. *El módulo M es la suma directa interna de los submódulos $M_1, \ldots, M_n$*
2. *$M = M_1 + \cdots + M_n$ y para cada i se verifica que $M_1 \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + m_n) = 0$*
3. *$M = M_1 + \cdots + M_n$ y para cada índice i se verifica $M_i \cap (M_1 + \cdots + M_{i-1}) = 0$*

En breve, $M$ es la suma directa de sus submódulos $M_1, \ldots, M_n$ si y sólo si $M = M_1 + \cdots + M_n$ y los submódulos son independientes.

**Teorema 6.4.15.** *Sea $M = \bigoplus_{i=1}^{n} M_i$.*

1. *Definimos los submódulos $N_1 = M_1 + \cdots + M_{r_1}$, $N_2 = M_{r_1+1} + \cdots + M_{r_1+r_2}$,etc. Entonces $M = \bigoplus N_j$.*
2. *Por su parte, si $M_i = \bigoplus_{j=1}^{r_i} M_{ij}$ para $i = 1, \ldots, n$ entonces $M = \bigoplus_{i,j} M_{ij}$.*

## 6.5. Matrices sobre un anillo

El alumno debe estar ya familiarizado con matrices y determinantes por el estudio del álgebra lineal. El objetivo de esta sección es generalizar estos conceptos a los contextos necesarios en el desarrollo posterior: Matrices con coeficientes en un anillo y determinantes de matrices con coeficientes en un anillo *conmutativo*. En resumen veremos que los resultados para matrices con coeficientes en un cuerpo se transportan *mutatis mutande*.

Sea $R$ un anillo arbitrario y sean $m, n$ enteros positivos.

**Definición 6.5.1.** Llamamos *matriz $m \times n$con coeficientes (elementos, entradas, coordenadas) en $R$* a toda tabla rectangular

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

El elemento $a_{ij}$ que está en la intersección de la fila $i$ con la columna $j$ se llama la *entrada* $(i, j)$ de la matriz. Dos matrices $A$ y $B = (b_{ij})$ son iguales si y sólo si para todo par $i, j$ se verifica $a_{ij} = b_{ij}$.

El conjunto de todas la matrices $m \times n$ con coeficientes en $R$ se denota como $M_{m\times n}(R)$.

**Definición 6.5.2.** Definimos la suma de matrices por coeficientes:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \cdots & a_{mn}+b_{mn} \end{pmatrix}$$

y el producto de una matriz $m \times n$ por una matriz $n \times s$ por la fórmula usual:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1s} \\ b_{21} & b_{22} & \cdots & b_{2s} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{ns} \end{pmatrix} = \begin{pmatrix} \sum_k a_{1k}b_{k1} & \sum_k a_{1k}b_{k2} & \cdots & \sum_k a_{1k}b_{ks} \\ \sum_k a_{2k}b_{k1} & \sum_k a_{2k}b_{k2} & \cdots & \sum_k a_{2k}b_{ks} \\ \cdots & \cdots & \cdots & \cdots \\ \sum_k a_{mk}b_{k1} & \sum_k a_{mk}b_{k2} & \cdots & \sum_k a_{mk}b_{ks} \end{pmatrix}$$

Denotamos com $1 = I = I_n$ a la *matriz identidad*, es decir la matriz $n \times n$ siguiente:

$$1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

**Teorema 6.5.3.** *1. La suma de matrices es asociativa, conmutativa, tiene como elemento neutro a la matriz cero y toda matriz tiene opuesto para la suma.*

*2. El conjunto $M_{m\times n}(R)$ es un grupo abeliano para la suma*

*3. El producto de matrices es asociativo, distributivo respecto a la suma y tiene como elemento neutro a la matriz identidad correspondiente.*

*4. El conjunto $M_n(R)$ de todas las matrices cuadradas $n \times n$ con coeficientes en $R$ es un anillo para la suma y producto anteriores.*

**Definición 6.5.4.** El grupo de matrices invertibles de $M_n(R)$ se llama *grupo lineal general* sobre $R$ y se denota por $GL_n(R)$.

**Definición 6.5.5.** Dos matrices $A, B \in M_{m\times n}(R)$ se llaman *equivalentes* si existen matrices invertibles $P \in M_m(R)$, $Q \in M_n(R)$ tales que $B = PAQ$.

**Lema 6.5.6.** *La relación anterior es una relación de equivalencia en* $M_{m\times n}(R)$.

**Definición 6.5.7.** Dos matrices cuadradas $A, B \in M_m(R)$ se llaman *semejantes* si existe una matriz invertible $P \in M_m(R)$ tal que $B = P^{-1}AP$.

**Lema 6.5.8.** *La relación de semejanza es una relación de equivalencia en* $M_m(R)$.

**Definición 6.5.9.** Sea $R$ un anillo *conmutativo*. Para toda matriz cuadrada $n \times n$ $A = (a_{ij})$ llamamos *determinante de* $A$ al elemento de $R$ definido por

$$\det(A) = \sum_{\sigma} sig(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$$

donde la suma se toma sobre todas las permutaciones $\sigma$ del conjunto $\{1, 2, \dots, n\}$ y $sig(\sigma)$ es el signo de $\sigma$ (que vale 1 si $\sigma$ es par y $-1$ cuando $\sigma$ es impar).

**Lema 6.5.10.** *Para matrices* $A, B \in M_n(R)$ *se verifica*

$$\det(AB) = \det(A)\det(B)$$

**Definición 6.5.11.** El *cofactor* $A_{ij}$ del coeficiente $a_{ij}$ de la matriz $A$ se define como $(-1)^{i+j}$ por el determinnate de la matriz $(n-1)\times(n-1)$ que se obtiene eliminando la fila $i$ y la columna $j$ de la matriz $A$.

**Definición 6.5.12.** Llamamos *adjunta* de la matriz $A = (a_{ij})$ a la matriz $\text{adj}(A) = (A_{ij})$.

**Lema 6.5.13.** 1. *Para todo* $i$ *se verifica* $\det(A) = a_{i1}A_{i1} + \cdots + a_{in}A_{in}$

2. *Para todo* $j$ *se verifica* $\det(A) = a_{1j}A_{1j} + \cdots + a_{nj}A_{nj}$

3. *Se verifica la igualdad de matrices:*

$$A \cdot (\text{adj}(A)) = \det(A) \cdot I = (\text{adj}(A)) \cdot A$$

**Teorema 6.5.14.** *Sea* $R$ *un anillo conmutativo. Una matriz* $A \in M_n(R)$ *es invertible si y sólo si* $\det(A)$ *es invertible en* $R$.

La inversa de $A$ se obtiene por la regla habitual: *La matriz* $A^{-1}$ *es igual a la adjunta de la traspuesta dividida por el determinante.*

**Corolario 6.5.15.** *Sea* $F$ *un cuerpo. Una matriz* $A \in M_n(F)$ *es invertible si y sólo si* $\det(A) \neq 0$.

**Proposición 6.5.16.** *Sea* $R$ *un anillo conmutativo*

1. *Sean* $A, B \in M_{m\times m}(R)$. *Entonces* $AB = I_m$ *si y sólo* $BA = I_n$.

2. *Sean* $A \in M_{m\times n}(R)$, $B \in M_{n\times m}(R)$ *tales que* $AB = I_m$. *Entonces* $m \leq n$.

3. *Sean* $A \in M_{m\times n}(R)$, $B \in M_{n\times m}(R)$ *tales que* $AB = I_m$ *y* $BA = I_n$. *Entonces* $m = n$.

*Demostración.* 1. La igualdad $AB = I$ implica que $\det(A)\det(B) = 1$. Por el teorema anterior $A$ es invertible y $A^{-1} = B$. Luego $BA = A^{-1}A = I_n$.

2. Supongamos que $m > n$. Descomponemos en bloques:

$$A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}, \qquad B = \begin{pmatrix} B_1 & B_2 \end{pmatrix}$$

donde $A_1, B_1 \in M_n(R)$ y $A_2, B_2 \in M_{(m-n)\times n}(R)$. Calculando el producto

$$AB = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}\begin{pmatrix} B_1 & B_2 \end{pmatrix} = \begin{pmatrix} A_1B_1 & A_1B_2 \\ A_2B_1 & A_2B_2 \end{pmatrix} = I_m$$

Como $A_1$ es cuadrada, sabemos que $B_1 = A_1^{-1}$ y $B_1A_1 = I_n$. Calculamos el producto

$$\begin{aligned} \begin{pmatrix} I_n & 0 \\ 0 & I_{m-n} \end{pmatrix} &= \begin{pmatrix} B_1 & 0 \\ 0 & I_{m-n} \end{pmatrix}\begin{pmatrix} I_n & 0 \\ 0 & I_{m-n} \end{pmatrix}\begin{pmatrix} A_1 & 0 \\ 0 & I_{m-n} \end{pmatrix} \\ &= \begin{pmatrix} B_1 & 0 \\ 0 & I_{m-n} \end{pmatrix}\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}\begin{pmatrix} B_1 & B_2 \end{pmatrix}\begin{pmatrix} A_1 & 0 \\ 0 & I_{m-n} \end{pmatrix} \\ &= \begin{pmatrix} B_1A_1 \\ A_2 \end{pmatrix}\begin{pmatrix} B_1A_1 & B_2 \end{pmatrix} = \begin{pmatrix} I_n \\ A_2 \end{pmatrix}\begin{pmatrix} I_n & B_2 \end{pmatrix} \\ &= \begin{pmatrix} I_n & B_2 \\ A_2 & A_2B_2 \end{pmatrix} \end{aligned}$$

lo que demuestra que $A_2 = 0$, $B_2 = 0$ y $A_2B_2 = I_{m-n} \neq 0$, lo que es una contradicción. Luego siempre $m \leq n$.

3. El párrafo anterior muestra que $m \leq n$. Cambiando los papeles de $B$ y $A$ obtenemos que $n \leq m$ y por tanto $m = n$.

□

*Observación* 6.5.17. Si el anillo $R$ no es conmutativo, la proposición 6.5.16 no tiene que ser cierta. Veamos un ejemplo de matrices $A \in M_{1\times 2}(R)$ y $B \in M_{2\times 1}(R)$ tales que $AB = I_1 = 1$ y $BA = I_2$, luego en este caso $m \neq n$:

Sea $F$ un cuerpo arbitrario y sea $V$ un espacio vectorial sobre $F$ de dimensión infinita numerable. Sea $\mathcal{B} = \{u_1, u_2, \dots\}$ una base para $V$ sobre $F$.

El anillo que vamos a considerar es $\mathrm{End}_F(V)$, el anillo de endomorfismos de $V$. Cualquier elemento de $R$ está totalmente determinado por las imágenes de los elementos de la base, así que definimos cuatro elementos $f_1, f_2, g_1, g_2 \in R$ de la siguiente manera:

$$\begin{aligned} f_1(u_i) &= u_{2i} \quad i = 1, 2, \dots \\ f_2(u_i) &= u_{2i-1} \quad i = 1, 2, \dots \\ g_1(u_i) &= \begin{cases} u_{i/2} & \text{cuando } i \equiv 0 \pmod 2 \\ 0 & \text{cuando } i \equiv 1 \pmod 2 \end{cases} \\ g_2(u_i) &= \begin{cases} 0 & \text{cuando } i \equiv 0 \pmod 2 \\ u_{(i+1)/2} & \text{cuando } i \equiv 1 \pmod 2 \end{cases} \end{aligned}$$

Es rutina comprobar que

$$\begin{aligned} g_1f_1 = g_2f_2 &= 1, \\ g_1f_2 = g_2f_1 &= 0 \\ f_1g_1 + f_2g_2 &= 1 \end{aligned}$$

(Sólo hay que comprobar las imágenes de los elementos de la base bajo cada una de estas aplicaciones). Formamos las matrices

$$A = \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}, \qquad B = \begin{pmatrix} f_1 & f_2 \end{pmatrix}$$

Un cálculo simple muestra que

$$AB = \begin{pmatrix} g_1 f_1 & g_1 f_2 \\ g_2 f_1 & g_2 f_2 \end{pmatrix} = I_2, \qquad BA = f_1 g_1 + f_2 g_2 = I_1$$

## 6.6. Módulos libres y matrices

**Definición 6.6.1.** Sea $F$ un $R$-módulo y $\mathcal{B} = \{v_1, \ldots, v_n\}$ un subconjunto de $F$. Decimos que $F$ *es libre sobre la base* $\mathcal{B}$ si para todo $x \in F$ existen únicos $a_1, \ldots, a_n \in R$ tales que $x = a_1 e_1 + \cdots + a_n e_n$.

Sea $R$ un anillo y sea $R^n = R \oplus R \oplus \cdots \oplus R$ ($n$ veces). Para $i = 1, \ldots, n$ llamamos

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

(el uno en el lugar $i$). Entonces

$$(x_1, x_2, \ldots, x_n) = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n$$

Luego los elementos $e_1, \ldots, e_n$ generan el módulo $R^n$. Además $\sum_i x_i e_i = \sum_i y_i e_i$ si y sólo si $x_i = y_i$ para todo $i = 1, \ldots, n$, así que $R^n$ es libre sobre la base $\{e_1, \ldots, e_n\}$, que se suele llamar la *base canónica* de $R^n$. Vamos a ver que en esencia este es el único $R$-modulo libre sobre una base con $n$ elementos:

**Teorema 6.6.2** (Propiedad universal de $R^n$)**.** *Sea $M$ un $R$-módulo cualquiera y sean $x_1, \ldots, x_n \in M$ arbitrarios. Existe un único homomorfismo de $R$-módulos $f : R^n \to M$ dado por $f(e_i) = x_i$ para $i = 1, \ldots, n$.*

**Corolario 6.6.3.** *Todo módulo se expresa como cociente de un módulo libre.*

**Definición 6.6.4.** Una *presentación* para un módulo $M$ es un módulo libre $F$ y un submódulo suyo $K$ tales que $M \cong F/K$.

El submódulo $K$ se llama *núcleo definidor* de $M$

Cuando ambos $F$ tiene una base finita $\{e_1, \ldots, e_n\}$ y $K$ es finitamente generado por $\{f_1, \ldots, f_m\}$ donde $f_j = \sum_i a_{ij} e_i$ y $e_i \mapsto u_i \in M$, la presentación se llama *finita* y la denotamos igual que para grupos abelianos:

$$M = \langle u_1, \ldots, u_n \mid \sum_i a_{ij} u_j = 0, \quad j = 1, \ldots, m \rangle$$

**Corolario 6.6.5.** *Si $M$ es libre sobre la base $\{x_1, \ldots, x_n\}$, existe un isomorfismo $R^n \cong M$ dado por $f(e_i) = x_i$ para $i = 1, \ldots, n$.*

**Teorema 6.6.6.** *Si $R$ es un anillo conmutativo, $R^m \cong R^n$ si y sólo si $m = n$.*

*Demostración.* Sean $R^m \cong M \cong R^n$ y sean $\{e_1, \ldots, e_m\}$ y $\{f_1, \ldots, f_n\}$ dos bases de $M$. Entonces existen $a_{ji}, b_{ij} \in R$ tales que

$$f_j = \sum_{i=1}^{m} a_{ji} e_i, \qquad e_i = \sum_{j=1}^{n} b_{ij} f_j \tag{6.6.1}$$

Sustituyendo cada una de las anteriores igualdades en la otra obtenemos:

$$f_j = \sum_{i=1}^{m}\sum_{k=1}^{n} a_{ji}b_{ik}f_k, \qquad e_i = \sum_{j=1}^{n}\sum_{k=1}^{m} b_{ij}a_{jk}e_k$$

Ya que los $e_i$ y los $f_j$ forman bases, debe ser

$$\sum_{i=1}^{m} a_{ji}b_{ik} = \begin{cases} 1 & \text{si } j = k \\ 0 & \text{si } j \neq k \end{cases} \tag{6.6.2}$$

$$\sum_{j=1}^{n} b_{ij}a_{jk} = \begin{cases} 1 & \text{si } i = k \\ 0 & \text{si } i \neq k \end{cases} \tag{6.6.3}$$

Formamos las matrices

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ \dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & b_{nm} \end{pmatrix}$$

Las condiciones 6.6.2 y 6.6.3 son equivalentes a las ecuaciones matriciales $AB = I_m$ y $BA = I_n$. Ya que $R$ es conmutativo, esto implica que $m = n$. □

**Definición 6.6.7.** Sea $R$ un anillo conmutativo y $M \cong R^n$ un $R$-módulo libre. Al entero (único) $n$ le llamamos *rango de M*.

Las expresiones 6.6.1 y la demostración del teorema 6.6.6 se pueden reformular: Dados dos módulos libres $F_1 \cong R^n$ y $F_2 \cong R^m$ con bases respectivas $\mathcal{B}_1 = \{f_1, \dots, f_n\}$ y $\mathcal{B}_2 = \{e_1, \dots, e_m\}$, todo homomorfismo $\sigma : F_1 \to F_2$ está totalmente determinado por las imágenes de los elementos de la base $\mathcal{B}_1$:

$$\sigma(f_j) = \sum_{i=1}^{m} a_{ji}e_i$$

Para cualquier vector $x = \sum_j b_j f_j \in F_1$ tenemos que

$$\sigma(x) = \sigma\left(\sum_j b_j f_j\right) = \sum_j b_j\sigma(f_j) = \sum_i\sum_j a_{ji}b_j e_i$$

Llamando $\sigma(x) = \sum_i c_i e_i$ la expresión anterior se escribe en términos matriciales se escribe como

$$\begin{pmatrix} c_1 \\ c_2 \\ \dots \\ c_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix}$$

Llamamos *matriz asociada a $\sigma$ respecto a las bases $\mathcal{B}_1$ y $\mathcal{B}_2$* a la matriz

$$M_{\mathcal{B}_1,\mathcal{B}_2}(\sigma) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Es fácil comprobar las siguientes propiedades:

**Proposición 6.6.8.** *1. Sean $\sigma_1, \sigma_2 : F_1 \to F_2$ dos homomorfismos de módulos. Entonces*

$$M_{\mathcal{B}_1,\mathcal{B}_2}(\sigma_1 + \sigma_2) = M_{\mathcal{B}_1,\mathcal{B}_2}(\sigma_1) + M_{\mathcal{B}_1,\mathcal{B}_2}(\sigma_2)$$

*2. Sean $F_1, F_2, F_3$ módulos libres con bases respectivas $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$. Sean $\sigma : F_1 \to F_2$ y $\tau : F_2 \to F_3$ homomorfismos entre ellos Entonces se verifica:*

$$M_{\mathcal{B}_1,\mathcal{B}_3}(\tau\sigma) = M_{\mathcal{B}_2,\mathcal{B}_3}(\tau) \cdot M_{\mathcal{B}_1,\mathcal{B}_2}(\sigma)$$

*3. Para la aplicación identidad $1 : F_1 \to F_1$ se verifica*

$$M_{\mathcal{B}_1,\mathcal{B}_1}(1) = I_n$$

**Proposición 6.6.9.** *1. Existe un isomorfismo de $R$-módulos $\mathrm{Hom}_R(F_1, F_2) \cong M_{m\times n}(R)$ dado por*

$$\sigma \mapsto M_{\mathcal{B}_1,\mathcal{B}_2}(\sigma)$$

*2. Existe un isomorfismo de anillos $\mathrm{End}_R(F_1) \cong M_n(R)$ dado por*

$$\sigma \mapsto M_{\mathcal{B}_1,\mathcal{B}_1}(\sigma)$$

*Observación* 6.6.10. Las correspondencias de la proposición anterior no son canónicas, sino que dependen de las bases elegidas para los módulos libres $F_i$. De cualquier forma dotan a las matrices de una interpretación que se conoce como *interpretación alibi* ("otro lugar").

Sean ahora $\mathcal{B}_1 = \{u_1, \ldots, u_n\}$ y $\mathcal{B}_2 = \{u'_1, \ldots, u'_n\}$ dos bases del mismo módulo libre $F$ de rango $n$. A la aplicación identidad $1 : F \to F$ le corresponde una matriz cuadrada invertible, $P = \mathcal{M}_{\mathcal{B}_1,\mathcal{B}_2}(1) = (p_{ij})$ que es la *matriz de cambio de base* de $\mathcal{B}_1$ a $\mathcal{B}_2$. Esta es la *interpretación alias* ("otro nombre").

Obsérvese que para $j = 1, \ldots, n$, $u_j = \sum_j p_{ij} u'_i$, es decir que *la $j$-ésima columna de $P$ está compuesta por las coordenadas del $j$-ésimo vector de la base antigua en expresado en la base nueva*

Consideramos ahora un homomorfismo $\sigma : F_1 \to F_2$ entre dos $R$-módulos libres de rangos respectivos $n$ y $m$. Sean $\mathcal{B}_1 = \{f_1, \ldots, f_n\}$, $\mathcal{B}'_1 = \{f'_1, \ldots, f'_n\}$ dos bases para $F_1$ con matriz de cambio $Q = \mathcal{M}_{\mathcal{B}_1,\mathcal{B}'_1}(1) = (q_{ij})$ y sean $\mathcal{B}_2 = \{e_1, \ldots, e_m\}$ y $\mathcal{B}'_2 = \{e'_1, \ldots, e'_m\}$ con matriz de cambio $P = \mathcal{M}_{\mathcal{B}_2,\mathcal{B}'_2}(1) = (p_{ij})$. Sean $A = \mathcal{M}_{\mathcal{B}_1,\mathcal{B}_2}(1) = (a_{ij})$ y $A' = \mathcal{M}_{\mathcal{B}'_1,\mathcal{B}'_2}(1) = (a'_{ij})$.

Por la proposición 6.6.8 se verifica que $A = P^{-1}A'Q$

En el caso particular en que $F_1 = F_2$, $\mathcal{B}_1 = \mathcal{B}_2$ y $\mathcal{B}'_2 = \mathcal{B}'_2$ tenemos que $Q = P$ y $A = P^{-1}A'P$. En resumen,

**Proposición 6.6.11.** *1. Dos matrices $A, A' \in M_{m\times n}(R)$ son equivalentes si y sólo si están asociadas al mismo homomorfismo respecto a distintas bases.*

*2. Dos matrices $A, A' \in M_n(R)$ son semejantes si y sólo si están asociadas al mismo endomorfismo respecto a distintas bases.*

## 6.7. Módulos finitamente generados sobre un dominio euclídeo

Vamos ya a concentrarnos en nuestro objeto fundamental de estudio: Los módulos sobre un dominio de ideales principales.

**Teorema 6.7.1.** *Sea $R$ un DIP y sea $F = R^n$ un módulo libre de rango $n$. Todo submódulo de $F$ es libre de rango $m \leq n$.*

*Demostración.* Inducción sobre $n$. Para $n = 1$, $F \cong R$ y todo submódulo $I$ de $R$ es un ideal principal.

Si $I = 0$ es libre de rango 0. Si $I \neq 0$, es un ideal $I = Ra$ con $a \neq 0$; la aplicación $R \to I$ dada por $x \mapsto xa$ es un isomorfismo de $R$-módulos y por tanto $I \cong R$ es libre de rango 1.

Sea ahora $n > 1$ y suponemos el teorema cierto para todo módulo libre de rango menor que $n$. Sea $\{e_1, \ldots, e_n\}$ una base para $F$ y sea $F_1$ el submódulo generado por $\{e_2 \ldots, e_n\}$. Entonces $F_1$ es libre de rango $n-1$ y $F/F_1$ es libre de rango 1, con base $\{e_1 + F_1\}$. Sea $K$ un submódulo de $F$. Si $K \subset F_1$, por la hìpótesis de inducción el módulo $K$ es libre de rango menor o igual a $n-1$.

Si $K \not\subset F_1$, el módulo cociente $\bar{K} = (K + F_1)/F_1$ es un submódulo no nulo de $F/F_1$, luego es libre de rango 1. Sea $v + F_1$ un generador de $\bar{K}$ y sean $K_0 = \langle v \rangle$, $K_1 = K \cap F_1$. El módulo $K_0$ es libre de rango 1 y el módulo $K_1$ es libre de rango $m_1 \leq n-1$. Es fácil comprobar que $K = K_0 + K_1$ y $K_0 \cap K_1 = 0$. Luego $K = K_0 \oplus K_1 \cong R^{m_1+1}$, luego $K$ es libre de rango $m = m_1 + 1 \leq (n-1) + 1 = n$. □

Cuando $R$ es un cuerpo (cuyos único ideales son 0 y 1), el teorema anterior se especializa al resultado bien conocido de que si $V$ es un espacio vectorial de dimensión finita $n$, todo subespacio $W$ de $V$ tiene dimensión menor o igualque $n$.

**Corolario 6.7.2.** *Sea $M$ un $R$-módulo generado por $n$ elementos. Todo submódulo $N$ de $M$ tiene un conjunto de generadores con $m \leq n$ elementos.*

**Corolario 6.7.3.** *Sea $R$ un dominio de ideales principales. Todo $R$-módulo finitamente generado tiene una presentación finita.*

Este corolario nos dice que dado un $R$-módulo finitamente generado $M$ existe un homomorfismo

$$\sigma : R^n \to R^m$$

tal que $M \cong R^m / \operatorname{Im}(\sigma)$.

Esto nos lleva al problema de elegir bases adecuadas para $R^n$ y $R^m$ para que la matriz de $\sigma$ nos de una forma particularmente sencilla de las relaciones (i.e., los elementos de $\operatorname{Im}(\sigma)$, y aplicando la proposición 6.4.7 obtengamos la estructura para $M$.

## 6.8. Equivalencia de matrices sobre un dominio euclídeo

Sea $R$ un dominio euclídeo respecto a la función $\phi : R - \{0\} \to \mathbb{Z}^+$.

El problema que consideramos es seleccionar entre las matrices equivalentes a una matriz $A$ dada, una que tenga una forma "normal" sencilla.

Vamos a obtener las matrices $P, Q$ que transforman $A$ en una matriz en forma normal como producto de matrices de unos tipos especiales que definimos ahora:

Llamamos $e_{ij}$ a la matriz con coeficiente 1 en el lugar $(i, j)$ y 0 en todos los demás. Llamamos $I$ a la matriz identidad.

Obsérvese que $I = e_{11} + \cdots + e_{ii} + \ldots$.

**Definición 6.8.1.** Una *matriz elemental* es una matriz cuadrada de uno de los siguientes tipos:

1. Para todo $b \in R$ y todo par de índices $i \neq j$ la matriz

$$T_{ij}(b) = I + be_{ij}$$

se llama *matriz elemental de tipo I*.

2. Para $u \in R^\times = U(R)$ y todo índice $i$, la matriz

$$D_i(u) = I + (u-1)e_{ii}$$

se llama *matriz elemental de tipo II*.

3. Para todo par de índices $i \neq j$, la matriz

$$P_{ij} = I - e_{ii} - e_{jj} + e_{ij} + e_{ji}$$

se llama *matriz elemental de tipo III*.

**Lema 6.8.2.** *Las matrices elementales son invertibles. Explícitamente,*

$$T_{ij}(b)^{-1} = T_{ij}(-b), \qquad D_i(u)^{-1} = D_i(u^{-1}), \qquad P_{ij}^{-1} = P_{ij}$$

**Definición 6.8.3.** La multiplicación por la izquierda de una matriz $A$ por una matriz elemental de tipo I (II, III) se llama *transformación elemental por filas de tipo I (II, III)* de la matriz $A$.

La multiplicación por la derecha de una matriz $A$ por una matriz elemental de tipo I (II, III) se llama *transformación elemental por columnas de tipo I (II, III)* de la matriz $A$.

Sea una matriz $m \times n$.

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

**Lema 6.8.4.** *1. Una transformación elemental por filas de tipo I sustituye $A$ por la matriz*

$$A' = T_{ij}(b)A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a'_{i1} & \dots & a'_{in} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

*donde $a'_{ik} = a_{ik} + ba_{jk}$ para $k = 1, \dots n$*

*2. Una transformación elemental por filas de tipo II sustituye $A$ por la matriz*

$$A' = D_i(u)A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a'_{i1} & \dots & a'_{in} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

*donde $a'_{ik} = ua_{ik}$ para $k = 1, \dots n$*

*3. Una transformación elemental por filas de tipo III sustituye $A$ por la matriz*

$$A' = P_{ij}A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a'_{i1} & \dots & a'_{in} \\ \dots & \dots & \dots \\ a'_{j1} & \dots & a'_{jn} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

*donde $a'_{ik} = a_{jk}$ y $a'_{jk} = a_{ik}$ para $k = 1, \dots n$*

**Lema 6.8.5.** *1. Una transformación elemental por columnas de tipo I sustituye A por la matriz*

$$A' = AT_{ij}(b) = \begin{pmatrix} a_{11} & \dots & a'_{1j} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a'_{mj} & \dots & a_{mn} \end{pmatrix}$$

*donde* $a'_{kj} = a_{kj} + ba_{ki}$ *para* $k = 1, \dots m$

2. *Una transformación elemental por columnas de tipo II sustituye A por la matriz*

$$A' = AD_i(u) = \begin{pmatrix} a_{11} & \dots & a'_{1i} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a'_{mi} & \dots & a_{mn} \end{pmatrix}$$

*donde* $a'_{ki} = ua_{ki}$ *para* $k = 1, \dots m$

3. *Una transformación elemental por columnas de tipo III sustituye A por la matriz*

$$A' = AP_{ij} = \begin{pmatrix} a_{11} & \dots & a'_{1i} & \dots & a'_{1j} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a'_{mi} & \dots & a'_{mj} & \dots & a_{mn} \end{pmatrix}$$

*donde* $a'_{ki} = a_{kj}$ *y* $a'_{kj} = a_{ki}$ *para* $k = 1, \dots m$

**Lema 6.8.6.** *Las matrices que se obtienen a partir de A por transformaciones elementales de filas o columnas son equivalentes a la matriz A.*

**Proposición 6.8.7.** *Sea A una matriz* $m \times n$ *con coeficientes en R. Existen matrices* $P_0, Q_0$ *invertibles sobre R de órdenes respectivos* $m, n$ *tales que*

$$P_0AQ_0 = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & b_{m2} & \dots & b_{mn} \end{pmatrix}$$

*donde* $d_1 \geq 0$ *y* $d_1 \mid b_{ij}$ *para todo par* $i, j$.

*Demostración.* Si $A = 0$ es la matriz cero, no hay nada que demostrar.

Si $A \neq 0$, sea $a_{ij}$ un elemento no nulo con $\phi(a)$ mínimo. Mediante transformaciones elementales de filas y columnas podemos llevar este elemento a la posición $(1, 1)$.

Sea $k > 1$ y sea $a_{1k} = a_{11}b_k + b_{1k}$ con $\phi(b_{1k}) < \phi(a_{11})$. Restamos la primera columna multiplicada por $b_k$ de la $k$-ésima. Esta transformación elemental reemplaza $a_{1k}$ por $b_{1k}$. Si $b_{1k} \neq 0$ obtenemos una matriz equivalente a la matriz $A$ para la que el mínimo de los valores $\phi(a_{ik})$ de los coeficientes no nulos es estrictamente menor que el de $A$. Repetimos el procedimiento original con esta matriz.

De la misma forma, si $a_{k1} = a_{11}b_k + b_{k1}$ con $0 < \phi(b_{k1}) < \phi(a_{11})$, una transformación elemental por filas de tipo I proporciona una matriz equivalente para la que el mínimo de los valores $\phi(a_{ij})$ de los coeficientes es estrictamente menor que el de $A$. Ya que cada aplicación de este proceso disminuye dicho mínimo, un número finito de repeticiones nos lleva a una matriz $B = (b_{ij})$ equivalente con $A$ tal que $b_{11}$ divide a todos los $b_{1k}$ y todos los $b_{k1}$. Nuevas transformaciones elementales de tipo I de filas y de columnas dan una matriz equivalente con $A$ de la forma

$$\begin{pmatrix} b_{11} & 0 & \dots & 0 \\ 0 & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & c_{m2} & \dots & c_{mn} \end{pmatrix}$$

Si existe un $c_{ij}$ no divisible por $b_{11}$, sumamos la $i$-ésima fila a la primera con lo que obtenemos la nueva primera fila $(b_{11}, c_{i2}, \ldots, c_{in})$ con $b_{11} \nmid c_{ij}$. Repitiendo el primer proceso reemplazamos $c_{ij}$ por un nuevo elemento $c'_{ij}$ tal que $\phi(c'_{ij}) < \phi(b_{11})$.

Un número finito de pasos como los indicados darán finalmente la matriz buscada. □

**Teorema 6.8.8** (Forma normal de Smith para matrices sobre un dominio euclídeo)**.** *Sea $R$ un dominio euclídeo y sea $A$ una matriz $m \times n$ con coeficientes en $R$. Existen matrices $P, Q$ invertibles sobre $R$ de órdenes respectivos $m, n$ tales que*

$$PAQ = \begin{pmatrix} d_1 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d_r & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & \ldots & 0 \end{pmatrix}$$

*donde $d_i \mid d_{i+1}$ para todo $i$.*

*Demostración.* Inducción sobre el número de filas y columnas. Dada una matriz $A \in M_{m\times n}(R)$, la proposición 6.8.7 genera una matriz equivalente

$$\begin{pmatrix} d_1 & 0 \\ 0 & A_1 \end{pmatrix}$$

donde $A_1 \in M_{(m-1)\times(n-1)}(R)$ y todos los coeficientes de $A_1$ son divisibles por $d_1$. Por inducción, transformaciones elementales de filas y columnas transforman $A_1$ a una matriz

$$\begin{pmatrix} d_2 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & d_r & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & \ldots & 0 \end{pmatrix}$$

con $d_i \mid d_{i+1}$. □

**Definición 6.8.9.** El número $r$ de elementos no nulos en la diagonal de la forma normal de Smith de una matriz $A$ se llama *rango de $A$*.

Los ideales generados por los elementos no nulos $d_i$ en la diagonal se llaman *factores invariantes de la matriz $A$*.

**Teorema 6.8.10.** *Sea $A \in M_{m\times n}(R)$ de rango $r$. Para cada $i = 1, \ldots r$ sea $\Delta_i$ el máximo común divisor de los menores $i \times i$ de $A$. Entonces los factores invariantes de $A$ son los ideales generados por*

$$d_1 = \Delta_1, \quad d_2 = \Delta_2/\Delta_1, \quad \ldots \quad d_r = \Delta_r/\Delta_{r-1}$$

**Corolario 6.8.11.** *Los factores invariantes $d_i$ del teorema 6.8.8 están determinados de manera única por la matriz $A$.*

**Corolario 6.8.12.** *Dos matrices $A, B \in M_{m\times n}(R)$ son equivalentes si y sólo si tienen los mismos factores invariantes.*

**Proposición 6.8.13.** *Una matriz cuadrada $A \in M_{n\times n}(R)$ es invertible en $M_{n\times n}(R)$ si y sólo si su determinante es invertible.*

**Corolario 6.8.14.** *Una matriz cuadrada $A \in M_{n\times n}(R)$ es invertible en $M_{n\times n}(R)$ si y sólo si su rango vale $n$ y todos sus factores invariantes valen* (1)*.*

**Corolario 6.8.15.** *Una matriz cuadrada $A \in M_{n\times n}(R)$ es invertible en $M_{n\times n}(R)$ si y sólo si es un producto de matrices elementales.*

*Ejemplo* 6.8.16. Para ilustrar los procedimientos anteriores tomamos un ejemplo sencillo y realizamos paso a paso las reducciones. Sea $R = \mathbb{Q}[X]$ y sea $A$ la matriz

$$A = \begin{pmatrix} X+1 & 1 & 1 \\ 2 & X & 1 \\ -6 & -3 & X-4 \end{pmatrix}$$

Queremos reducirla a su forma normal de Smith. Desarrollamos el trabajo en forma tabular arrastrando los productos de transformaciones de filas a la izquierda y los productos de transformaciones de columnas a la derecha. La columna central empieza con $A$ y termina con $D$, la forma normal de Smith:

$$\begin{array}{ccc|ccc|ccc}
1 & 0 & 0 & X+1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 2 & X & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & -6 & -3 & X-4 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & 1 & X+1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & X & 2 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & -3 & -6 & X-4 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & X & -X^2-X+2 & -X+1 & 1 & -X-1 & -1 \\
0 & 0 & 1 & -3 & 3X-3 & X-1 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
-X & 1 & 0 & 0 & -X^2-X+2 & -X+1 & 1 & -X-1 & -1 \\
3 & 0 & 1 & 0 & 3X-3 & X-1 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
-X & 1 & 0 & 0 & -X+1 & -X^2-X+2 & 1 & -1 & -X-1 \\
3 & 0 & 1 & 0 & X-1 & 3X-3 & 0 & 1 & 0 \\
\hline
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
3 & 0 & 1 & 0 & X-1 & 3X-3 & 1 & -1 & -X-1 \\
-X & 1 & 0 & 0 & -X+1 & -X^2-X+2 & 0 & 1 & 0 \\
\hline
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
3 & 0 & 1 & 0 & X-1 & 3X-3 & 1 & -1 & -X-1 \\
-X+3 & 1 & 1 & 0 & 0 & -X^2+2X-1 & 0 & 1 & 0 \\
\hline
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
3 & 0 & 1 & 0 & X-1 & 0 & 1 & -1 & -X+2 \\
-X+3 & 1 & 1 & 0 & 0 & -X^2+2X-1 & 0 & 1 & -3 \\
\hline
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\
3 & 0 & 1 & 0 & X-1 & 0 & 1 & -1 & X-2 \\
-X+3 & 1 & 1 & 0 & 0 & X^2-2X+1 & 0 & 1 & 3
\end{array}$$

Los cálculos anteriores muestran que

$$\begin{pmatrix} 1 & 0 & 0 \\ 3 & 0 & 1 \\ -X+3 & 1 & 1 \end{pmatrix}\begin{pmatrix} X+1 & 1 & 1 \\ 2 & X & 1 \\ -6 & -3 & X-4 \end{pmatrix}\begin{pmatrix} 0 & 0 & -1 \\ 1 & -1 & X-2 \\ 0 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & 0 \\ 0 & 0 & X^2-2X+1 \end{pmatrix}$$

## 6.9. Teorema de estructura de módulos finitamente generados sobre un dominio euclídeo

**Teorema 6.9.1** (Descomposición cíclica canónica)**.** *Sea $R$ un dominio de ideales principales y sea $M$ un $R$-módulo finitamente generado. Entonces existen elementos $a_1, \dots, a_s \in R$ tales que*

$$M \cong R^r \oplus \frac{R}{Ra_1} \oplus \cdots \oplus \frac{R}{Ra_s}$$

*con $a_i \mid a_{i+1}$ para $i = 1, \dots, s-1$*

*Tal descomposición es única salvo isomorfismo.*

El número $r$ se llama *rango* de $M$y los elementos $a_1, \dots, a_s$ se llaman *factores invariantes de $M$*

## 6.10. Módulos de torsión y componentes primarias. Teorema de invarianza

Sea $M$ un $R$-módulo.

**Definición 6.10.1.** Un elemento $u \in M$ se llama *de torsión* si existe un elemento $a \in$ no nulo tal que $au = 0$.

El conjunto de todos los elementos de torsión de $M$ se llama *submódulo de torsión* y se representa por $\mathrm{Tor}(M)$.

**Proposición 6.10.2.** *El conjunto* $\mathrm{Tor}(M)$ *es un $R$-submódulo de $M$.*

**Definición 6.10.3.** Un módulo $M$ se llama *de torsión* si $\mathrm{Tor}(M) = M$, es decir, si todos sus elementos son de torsión.

Un módulo $M$ se llama *libre de torsión* si $\mathrm{Tor}(M) = 0$, es decir, si su único elemento de torsión es el cero.

**Teorema 6.10.4.** *Todo módulo finitamente generado sobre un DIP es suma directa de su submódulo de torsión con un módulo libre.*

**Corolario 6.10.5.** *Un módulo finitamente generado sobre un DIP es libre de torsión si y sólo si es libre.*

**Lema 6.10.6.**
1. *Sea $M = Rx$ con $\mathrm{Ann}(x) = Rd$ y $d = gh$ con $\mathrm{m.c.d.}(g,h) = 1$. Entonces $M = Ry \oplus Rz$ con $\mathrm{Ann}(y) = Rg$ y $\mathrm{Ann}(z) = Rh$.*
2. *Si $M = Ry + Rz$ con $\mathrm{Ann}(y) = Rg$, $\mathrm{Ann}(z) = Rh$ y $\mathrm{m.c.d.}(g,h) = 1$, entonces $M = Rx$ con $\mathrm{Ann}(x) = R \cdot gh$.*

**Definición 6.10.7.** Sea $p \in R$ un primo y sea $M$ un $R$-módulo. Un elemento $u \in M$ se llama *$p$-primario* si $\mathrm{Ann}(u) = (p^k)$.

Llamamos *componente $p$-primaria* de $M$ al conjunto de todos los elementos $p$-primarios. Se representa por $M_p$.

Un $R$-módulo $M$ se llama $p$-primario si $M = M_p$, es decir, si todos sus elementos son $p$-primarios.

**Lema 6.10.8.** *La componente $p$-primaria $M_p$ es un $R$-submódulo de $M$.*

**Teorema 6.10.9** (Descomposición primaria)**.** *Sea $R$ un DIP y sea $M$ un $R$-módulo de torsión finitamente generado. Entonces $M_p = 0$ todo primo $p$ excepto un número finito.*

*Sea $\{p \mid M_p \neq 0\} = \{p_1, \dots, p_k\}$. Entonces*

$$M = M_{p_1} \oplus \cdots \oplus M_{p_k}$$

**Teorema 6.10.10** (Descomposición cíclica primaria)**.** *Todo módulo de torsión finitamente generado $M$ es una suma directa de módulos cíclicos primarios:*

$$M = Rv_1 \oplus \cdots \oplus Rv_m$$

*con* $\mathrm{Ann}(x_i) = Rp_i^{k_i}$.

**Definición 6.10.11.** Los elementos $p_1^{k_1}, \ldots, p_m^{k_m}$ se llaman *divisores elementales* del módulo $M$.

**Lema 6.10.12.** *La lista de factores invariantes de $M$ determina unívocamente a la lista de divisores elementales de $M$ y viceversa.*

## 6.11. Aplicaciones a transformaciones lineales: Formas canónicas

Sea $F$ un cuerpo y sea $V$ un espacio vectorial sobre $F$ con base $\{u_1, \ldots, u_n\}$. Sea $t : V \to V$ una aplicación lineal. Escribimos

$$t(u_j) = \sum_{i=1}^{n} a_{ij} u_i, \qquad j = 1, \ldots, n$$

Entonces $A = (a_{ij})$ es la matriz asociada de $t$ respecto a la base dada.

Consideramos la estructura de $F[X]$-módulo definida sobre $M = V$ por $t$.

**Lema 6.11.1.** *El $F[X]$-módulo $M$ es un módulo de torsión.*

La $F$-base dada es un conjunto de generadores del $F[X]$-módulo $M$, aunque no es una base. Sea $\mathcal{B}_2 = \{e_1, \ldots, e_n\}$ la base canónica de $F[X]^n$. Existe un epimorfismo $\rho : F[X]^n \to M$ dado por $\rho(e_i) = u_i$. Llamamos $K = \ker(\rho)$. Sabemos que $M = \mathrm{Im}(\rho) \cong F[X]^n/K$. Vamos a obtener una base para $K$:

**Lema 6.11.2.** *El submódulo $K$ es libre con base $\mathcal{B}_1 = \{f_1, \ldots, f_n\}$ donde*

$$f_j = Xe_j - \sum_{i=1}^{n} a_{ij} e_i$$

La matriz de la inclusión $\sigma : K \to F[X]^n$ es

$$M_{\mathcal{B}_1, \mathcal{B}_2} = XI - a = \begin{pmatrix} X - a_{11} & -a_{12} & \ldots & -a_{1n} \\ -a_{21} & X - a_{22} & \ldots & -a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ -a_{n1} & -a_{n2} & \ldots & X - a_{nn} \end{pmatrix}$$

Luego esta matriz proporciona los factores invariantes del $F[X]$-módulo $M$ y por tanto, la descomposición de $M$ como suma directa de módulos cíclicos.

**Definición 6.11.3.** El determinante $g(X) = \det(XI - A) = X^n - a_{n-1}X^{n-1} + \cdots + (-1)^n a_0$ se llama *polinomio característico* de la matriz $A$.

El elemento $a_{n-1} = \sum a_{ii}$ se llama *traza* de la matriz $A$.

Obsérvese que $a_0 = \det(A)$. En general, el coeficiente $a_{n-i}$ es la suma de los menores $i \times i$ principales (=diagonales) de la matriz $A$. Como $g(X) \neq 0$ y $g(X)$ es el producto de los factores invariantes de $XI - A$,

es inmediato que $M$ es un módulo de torsión sobre $F[X]$. Así que la forma normal de Smith de $XI - A$ es

$$A' = \begin{pmatrix} 1 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & d_1(X) & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & d_s(X) \end{pmatrix}$$

donde los $d_i(X)$ son polinomios mónicos de grado positivo y se verifica $d_i(X) \mid d_{i+1}(X)$ para $i = 1, \dots, s-1$.

El teorema 6.8.8 muestra que existen matrices invertibles $P, Q$ con coeficientes en $F[X]$ tales que $A' = P^{-1}AQ$. Escribimos $P = (p_{ij})$ y definimos $e'_j = \sum_i p_{ij} e_i$, $j = 1, \dots, n$. Sus imágenes son $v_j = \rho(e'_j) \in M$. Finalmente renombramos $z_k = v_{n-s+k}$, $k = 1, \dots, s$ y tenemos

$$V = M = F[X]z_1 \oplus F[X]z_2 \oplus \cdots \oplus F[X]z_s \tag{6.11.1}$$

donde $\mathrm{Ann}(z_k) = (d_k(X))$. Sea $n_k = gr(d_k)$. En cada submódulo $F[X]z_k$ tomamos la $F$-base $\{z_k, Xz_k, \dots, X^{n_k-1}z_k\}$. La unión de todas estas bases,

$$\{z_1, Xz_1, \dots, X^{n_1-1}z_1, z_2, Xz_2, \dots, X^{n_2-1}z_2, \dots, z_s, Xz_s, \dots, X^{n_s-1}z_s\} \tag{6.11.2}$$

forman una base para $V$ sobre $F$.

**Proposición 6.11.4.** *La matriz asociada a $t$ respecto a la base 6.11.2 es*

$$B = \begin{pmatrix} B_1 & 0 & \dots & 0 \\ 0 & B_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & B_s \end{pmatrix}$$

*donde $B_k$ es la matriz asociada al polinomio $h_k$ para $k = 1, \dots, s$.*

**Definición 6.11.5.** La matriz de la proposición 6.11.4 se llama *forma canónica racional o de Frobenius* del endomorfismo $t$ y de la matriz $A$.

*Ejemplo* 6.11.6. Sea $V \cong \mathbb{Q}^3$ un espacio vectorial racional de dimensión 3 con base $\mathcal{B} = \{u_1, u_2, u_3\}$ y sea $T : V \to V$ la aplicación lineal dada por

$$\begin{aligned} T(u_1) &= -u_1 - 2u_2 + 6u_3 \\ T(u_2) &= -u_1 + 3u_3 \\ T(u_3) &= -u_1 - u_2 + 4u_3 \end{aligned}$$

La matriz de $T$ respecto a la base $\mathcal{B}$ es

$$A = \begin{pmatrix} -1 & -1 & -1 \\ -2 & 0 & -1 \\ 6 & 3 & 4 \end{pmatrix}$$

y la matriz característica es

$$XI - A = \begin{pmatrix} X+1 & 1 & 1 \\ 2 & X & 1 \\ -6 & -3 & X-4 \end{pmatrix}$$

En el ejemplo 6.8.16 hemos visto que

$$\begin{pmatrix} 1 & 0 & 0 \\ 3 & 0 & 1 \\ -X+3 & 1 & 1 \end{pmatrix}\begin{pmatrix} X+1 & 1 & 1 \\ 2 & X & 1 \\ -6 & -3 & X-4 \end{pmatrix}\begin{pmatrix} 0 & 0 & -1 \\ 1 & -1 & X-2 \\ 0 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & 0 \\ 0 & 0 & X^2-2X+1 \end{pmatrix}$$

luego los factores invariates de $V$ como $\mathbb{Q}[X]$-módulo son $X-1$ y $(X-1)^2 = X^2-2X+1$. Así que la forma canónica racional de $T$ es

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$$

Los cálculos del ejemplo 6.8.16 también proporcionan una base respecto a la que $T$ toma su forma canónica racional: Tenemos las matrices

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 3 & 0 & 1 \\ -X+3 & 1 & 1 \end{pmatrix}, \qquad P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ X & -1 & 1 \\ -3 & 1 & 0 \end{pmatrix}$$

así que $V$ está generado como $\mathbb{Q}[X]$-módulo por

$$\begin{aligned} v_1 &= u_1 + Xu_2 - 3u_3 \\ v_2 &= -u_2 + u_3 \\ v_3 &= u_2 \end{aligned}$$

La forma normal de Smith de $XI - A$ nos dice que $v_1 = 0$, $T(v_2) - v_2 = 0$, $T^2(v_3) - 2T(v_3) + v_3 = 0$.

Una $\mathbb{Q}$-base con respecto a la que $T$ toma su forma canónica racional es

$$\begin{aligned} z_1 &= v_2 = -u_2 + u_3 \\ z_2 &= v_3 = u_2 \\ z_3 &= T(v_3) = -u_1 + 3u_3 \end{aligned}$$

La matriz que relaciona esta base con la base inicial es

$$S = \begin{pmatrix} 0 & 0 & -1 \\ -1 & 1 & 0 \\ 1 & 0 & 3 \end{pmatrix}, \quad S^{-1} = \begin{pmatrix} 3 & 0 & 1 \\ 3 & 1 & 1 \\ -1 & 0 & 0 \end{pmatrix}$$

Es fácil comprobar que

$$S^{-1}AS = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$$

A partir de la descomposición 6.11.1 obtenemos la descomposición cíclica primaria del módulo $M$. Para ello descomponemos cada uno factor invariante:

$$d_i(X) = p_1^{k_{i1}} \dots p_m^{k_{im}}$$

Para cada $j = 1, \dots, m$ definimos

$$h_{ij}(X) = d_i(X)/p_j^{k_{ij}}, \qquad z_{ij} = h_{ij}(X)z_i$$

**Lema 6.11.7.** *Tenemos la descomposición*

$$F[X]z_i = F[X]z_{i1} \oplus \cdots \oplus F[X]z_{im}$$

*y* $\mathrm{Ann}(z_{ij}) = (p_i^{k_{ij}})$.

Sustituyendo en 6.11.1 obtenemos ahora la descomposición cíclica primaria:

$$V = M = F[X]z_{11} \oplus F[X]z_{12} \oplus \cdots \oplus F[X]z_{sm} \tag{6.11.3}$$

donde $\mathrm{Ann}(z_{ij}) = (p_i^{k_{ij}})$ y los $p_i^{k_{ij}}$ son los divisores elementales del módulo $M$. Llamamos $m_{ij} = gr(p_i^{k_{ij}}) = k_{ij}gr(p_i)$. Tomamos ahora la $F$-base de $V$ siguiente:

$$\{z_{11}, Xz_{11}, \ldots, X^{m_{11}-1}z_{11}, z_{12}, Xz_{12}, \ldots, X^{m_{12}-1}z_{12}, \ldots\} \tag{6.11.4}$$

**Proposición 6.11.8.** *La matriz asociada a $t$ respecto a la base 6.11.4 es*

$$B = \begin{pmatrix} B_{11} & 0 & \ldots & 0 \\ 0 & B_{12} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & B_{sm} \end{pmatrix}$$

*donde $B_{ij}$ es la matriz asociada al polinomio $p_i^{k_{ij}}$ para todo $i, j$.*

**Definición 6.11.9.** La matriz de la proposición 6.11.8 se llama *forma canónica racional primaria o de Weierstrass* del endomorfismo $t$ y de la matriz $A$.

*Ejemplo* 6.11.10. Sea $V \cong \mathbb{Q}^3$ un espacio vectorial racional de dimensión 3 con base canónica $\mathcal{B} = \{e_1, e_2, e_3\}$ y sea $T : V \to V$ la aplicación lineal que respecto a dicha base corresponde a la matriz

$$A = \begin{pmatrix} 4 & 2 & -4 \\ 2 & 3 & -3 \\ 3 & 2 & -3 \end{pmatrix}$$

Formamos la matriz

$$A_X = XI - A = \begin{pmatrix} X-4 & -2 & 4 \\ -2 & X-3 & 3 \\ -3 & -2 & X+3 \end{pmatrix}$$

Realizando los cálculos pertinentes obtenemos que la forma normal de Smith de $A_X$ es

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & d_1(X) \end{pmatrix}$$

donde $d_1(X) = X^3 - 4X^2 + 5X - 2 = (X-1)^2(X-2)$ y matrices

$$P = \begin{pmatrix} -2 & 0 & 0 \\ X-3 & 2X-3 & 1 \\ -2 & X-1 & \frac{1}{2} \end{pmatrix}, \qquad Q = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 2 & X^2 - \frac{5}{2}X + 2 \\ 0 & 1 & \frac{1}{2}X - \frac{3}{2}X + 2 \end{pmatrix}$$

tales que $B = P^{-1}AQ$. Luego $M = F[X]z_1$ donde $z_1 = (0, 1, 1/2)$ (la última columna de $P$). La forma canónica racional de $A$ es

$$A_F = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & -5 \\ 0 & 1 & 4 \end{pmatrix}$$

y una base con respecto a la que a $T$ le corresponde la matriz $FA$ está formada por los vectores

$$v_1 = z_1 = (0,1,1/2),\ v_2 = Av_1 = (0,3/2,1/2),\ v_3 = Av_2 = (1,3,3/2)$$

que son las columnas de la matriz de cambio de base:

$$S = \begin{pmatrix} 0 & 0 & 1 \\ 1 & \frac{3}{2} & 3 \\ \frac{1}{2} & \frac{1}{2} & \frac{3}{2} \end{pmatrix}$$

Es fácil comprobar que $A_F = S^{-1}AS$.

Los divisores elementales de la matriz $A$ son los factores del único factor invariante, $d_1 = g \cdot h$ donde $g = (X-2)$, $h = (X-1)^2$. Llamando

$$z_{11} = hz_1 = T^2(z_1) - 2T(z_1) + z_1 = (1,1,1),$$
$$z_{12} = gz_1 = T(z_1) - 2z_1 = (0,-1/2,-1/2)$$

tenemos la descomposición primaria

$$M = F[X]z_{11} \oplus F[X]z_{12}$$

donde el primer módulo es un espacio vectorial de dimensión 1 y el segundo tiene dimensión dos. Formamos los vectores de la base

$$u_1 = z_{11},\ u_2 = z_{12},\ u_3 = Xu_2 = T(u_2) = (1,0,1/2)$$

La matriz de cambio de la base canónica a la base calculada es

$$T = \begin{pmatrix} 1 & 0 & 1 \\ 1 & -\frac{1}{2} & 0 \\ 1 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

y la forma canónica de Weierstrass de la matriz $A$ dada es

$$A_W = T^{-1}AT = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$$

Podemos elegir una tercera base de $V$ sobre $F$:

$$\{z_{111}, z_{112}, \ldots, z_{11m_{11}}, z_{121}, z_{122}, \ldots, z_{12m_{12}}, \ldots\} \tag{6.11.5}$$

donde $z_{ijk} == (X^r p^q) \cdot z_{ij}$, siendo $k - 1 = q \cdot gr(p_i) + r$ con $0 \leq r < gr(p_i)$.

**Proposición 6.11.11.** *La matriz asociada a t respecto a la base 6.11.5 es*

$$B = \begin{pmatrix} J_{11} & 0 & \ldots & 0 \\ 0 & J_{12} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & J_{sm} \end{pmatrix}$$

*donde $J_{ij}$ es el bloque de Jacobson asociado al polinomio $p_i^{k_{ij}}$ para todo $i$, $j$.*

**Definición 6.11.12.** La matriz de la proposición 6.11.8 se llama *forma canónica de Jacobson* del endomorfismo $t$ y de la matriz $A$.

*Ejemplo* 6.11.13. En el ejemplo 6.11.6, los divisores elementales coiniden con los factores invariantes, por lo que las formas canónicas racional y de Weierstrass coinciden. La forma canónica de Jacobson es

$$A_J = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

y la base con respecto a la que a la aplicación $t$ le corresponde esta matriz es

$$w_1 = v_2 = (0, -1, 1),\ w_2 = v_3 = (0, 1, 0),\ w_3 = (X - 1)(w_2) = Av_3 - v_3 = (-1, -1, 3)$$

así que la matriz de cambio de base es

$$J = \begin{pmatrix} 0 & 0 & -1 \\ -1 & 1 & -1 \\ 1 & 0 & 3 \end{pmatrix}$$

Es fácil comprobar que $J^{-1}AJ = A_J$.

*Ejemplo* 6.11.14. Volviendo al ejemplo 6.11.10, la tercera base está formada por los vectores

$$w_1 = z_{11},\ w_2 = z_{12},\ w_3 = (X - 1)z_{12} = Aw_2 - w_2 = (1, 1/2, 1)$$

La matriz de cambio de base es ahora

$$J = \begin{pmatrix} 1 & 0 & 1 \\ 1 & -\frac{1}{2} & \frac{1}{2} \\ 1 & -\frac{1}{2} & 1 \end{pmatrix}$$

y la forma canónica de Jacobson de la matriz $A$ original es

$$A_J = J^{-1}AJ = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

En el caso particular en que todo los $p_i = X - a_i$ son de grado uno, la base 6.11.5 toma una forma particularmente sencilla:

$$\{z_{11}, (X - a_1)z_{11}, \ldots, (X - a_1)^{m_{11}-1}z_{11}, z_{12}, (X - a_2)z_{12}, \ldots, (X - a_2)^{m_{12}-1}z_{11}, \ldots\} \tag{6.11.6}$$

**Proposición 6.11.15.** *La matriz asociada a $t$ respecto a la base 6.11.6 es*

$$B = \begin{pmatrix} J_{11} & 0 & \ldots & 0 \\ 0 & J_{12} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & J_{sm} \end{pmatrix}$$

*donde para todo $i, j$*

$$J_{ij} = \begin{pmatrix} a_i & 0 & \ldots & 0 & 0 \\ 1 & a_i & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_i & 0 \\ 0 & 0 & \ldots & 1 & a_i \end{pmatrix}$$

*es el bloque de Jordan asociado al polinomio $(X - a_i)^{k_{ij}}$*

**Definición 6.11.16.** La matriz de la proposición 6.11.15 se llama *forma canónica de Jordan* del endomorfismo $t$ y de la matriz $A$.

## 6.12. Ejercicios

**Ejercicio 6.1.** Calcular los factores invariantes de las siguientes matrices sobre $\mathbb{Q}[x]$

$$\begin{pmatrix} x & 0 & 0 \\ 0 & 1-x & 0 \\ 0 & 0 & 1-x^2 \end{pmatrix} \begin{pmatrix} 2-x-x^2 & x-x^2 & -1-x+2x^2 \\ 1-x^2 & 1-x^2 & -2+2x^2 \\ -x+x^2 & -1+x & 2-x-x^2 \end{pmatrix} \begin{pmatrix} 1-x & -1+x^2 & 1-x^2 \\ 0 & -1+x^2 & 1-x^2 \\ 1-x & 0 & -1+x^2 \end{pmatrix}.$$

¿algunas de ellas son equivalentes entre si?.

**Ejercicio 6.2.** Sea $R = \mathbb{Q}[X]$. Obtener una forma normal para las matrices:

1. $$\begin{pmatrix} X-7 & 2 & -1 \\ 2 & X-10 & 2 \\ -1 & 2 & X-7 \end{pmatrix}$$

2. $$\begin{pmatrix} X-17 & 8 & 12 & -14 \\ -46 & X+22 & 35 & -41 \\ 2 & -1 & X-4 & 4 \\ -4 & 2 & 2 & X-3 \end{pmatrix}$$

**Ejercicio 6.3.** Sea $R$ un dominio euclídeo y sea $A \in M_{m\times n}(R)$ una matriz. Demostrar que $A$ y su traspuesta $A^t$ tienen los mismos factores invariantes.

**Ejercicio 6.4.** Calcular los factores invariantes y los divisores elementales del endomorfismo $t : V \to V$, que sobre los vectores de una base $e_1, e_2, e_3$ de V está definido por

$$\begin{array}{rcrrr} t(e_1) & = & -e_1 & & \\ t(e_2) & = & 3a_1 & +e_2 & +2e_3 \\ t(e_3) & = & & & -e_3 \end{array}$$

¿Es posible encontrar una base en V respecto de la cual la matriz de t sea la siguiente

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

**Ejercicio 6.5.** Demostrar que el $K[X]$-módulo definido por una transformación lineal $t$ es cíclico si y sólo si tiene un único factor invariante y si y solo si el polinomio característico de $A$ es el polinomio mínimo de $A$.

**Ejercicio 6.6.** Sea $R = \mathbb{R}[X]$ y sea $M$ un $R$-módulo que es una suma directa de módulos cíclicos cuyos anuladores minimales son $(X-1)^3$, $(X^2+1)^2$, $(X-1)(X^2+1)^4$, $(X+2)(X^2+1)^2$. Determinar los divisores elementales y los factores invariantes de $M$.

**Ejercicio 6.7.** Verificar que el polinomio característico de la matriz

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & -2 & 0 & 1 \\ -2 & 0 & -1 & -2 \end{pmatrix}$$

es un producto de factores lineales en $\mathbb{Q}[X]$. Determinar las formas canónicas racional, racional primaria y de Jordan de $A$ en $M_4(\mathbb{Q})$. Encontrar matrices que transformen $A$ en sus formas canónicas.

**Ejercicio 6.8.** Una matriz M, definida sobre el cuerpo $\mathbb{Q}$, tiene la siguiente lista de factores invariantes: $(x+1, x^2+2x+1, x^4-x^2+2x^3-4x-2)$. ¿que tamaño tiene esa matriz?. ¿cuales son sus divisores elementales?. ¿Cual es el polinomio mínimo de tal matriz?, ¿y el polinomio característico?.

**Ejercicio 6.9.** Hallar las formas canónicas racional, racional primaria y de Jordan para la matriz

$$A = \begin{pmatrix} 4 & 2 & -4 \\ 2 & 3 & -3 \\ 3 & 2 & -3 \end{pmatrix} \in M_n(\mathbb{C})$$

Hallar las matrices que transforman $A$ en sus formas canónicas.

**Ejercicio 6.10.** Un $\mathbb{R}[x]$-módulo $V$ es isomorfo a un producto directo de módulos cíclicos cuyos anuladores minimales son respectivamente: $(x-1)^3, (x^2+1)^2, (x-1)(x^2+1)^4$ y $(x+2)(x^2-2)^2$. Determinar los divisores elementales y los factores invariantes de $V$ Repetir el ejercicio suponiendo que $V$ es un $\mathbb{Q}[x]$-módulo.

**Ejercicio 6.11.** Calcular las formas canónicas y las matrices del cambio de base de la siguiente matriz sobre los racionales

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 5 & 7 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

**Ejercicio 6.12.** Dada la matriz

$$A_X = \begin{pmatrix} X-1 & 1 & -1 \\ 1 & X-1 & 1 \\ -1 & 1 & X-1 \end{pmatrix} \in M_3(\mathbb{Q}[X])$$

su forma normal de Smith es

$$D_X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & X^2-3X \end{pmatrix}$$

Unas matrices invertibles $Q, P \in M_{3\times 3}(\mathbb{Q}[X])$ tales que $QA_XP = D_X$ son

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ -X+1 & 1 & 0 \\ X-2 & -1 & 1 \end{pmatrix}, \qquad P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & -1 \\ 0 & 1 & X-2 \end{pmatrix}$$

cuyas inversas son

$$Q^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ X-1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \qquad P^{-1} = \begin{pmatrix} X-1 & 1 & -1 \\ -X+2 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

1. Sea la matriz

$$A = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix} \in M_{3\times 3}(\mathbb{Q})$$

Calcular los factores invariantes y divisores elementales de $A$. Escribir explícitamente las formas canónicas de $A$. (Observación: Utilizar los cálculos anteriores).

2. Determinar matrices invertibles $S, T \in M_{3\times 3}(\mathbb{Q})$ tales que $S^{-1}AS$ y $T^{-1}AT$ sean las respectivas formas canónicas de $A$. (Observación: La matriz $A$ es la del apartado anterior).

**Ejercicio 6.13.** Consideremos $t : V \to V$, donde $V$ es un espacio vectorial real de dimensión 4, la aplicación lineal que respecto a una base $\{u_1, u_2, u_3, u_4\}$ de $V$ está dada por las igualdades:

$$\begin{array}{lcrrrr} t(u_1) & = & 3u_1 & +u_2 & & \\ t(u_2) & = & -4u_1 & -u_2 & & \\ t(u_3) & = & 6u_1 & +u_2 & +2u_3 & +u_4 \\ t(u_4) & = & -14u_1 & -5u_2 & -u_3 & \end{array}$$

- Describir la matriz característica del endomorfismo respecto a la base dada.
- Calcular matrices P y Q sobre $\mathbb{R}[x]$, invertibles, tales que P(xI-M(t))Q sea normal.
- Describir los factores invariantes y los divisores elementales del endomorfismo $t$. Describir como es la descomposición cíclica y cíclica primaria en sumas directas del $\mathbb{R}[x]$-módulo que define $t$.
- Describir la forma canónica racional del endomorfismo $t$.

**Ejercicio 6.14.** Describir todas las formas canónicas sobre $\mathbb{R}$ de una matriz cuyos divisores elementales son

$$(x^2 + 4x + 5)^2, (x - 2)^2, (x + 1)^2, (x + 2), (x + 2)^2$$

**Ejercicio 6.15.** Probar que dos matrices $3 \times 3$ sobre un cuerpo K son semejantes si, y solo si, tienen el mismo polinomio característico y el mismo polinomio mínimo. Dar un contraejemplo explícito a que tal cosa es falsa para matrices $4 \times 4$.

**Ejercicio 6.16.** Razona que una matriz cuadrada ( o un endomorfismo) sobre un cuerpo K es diagonalizable por semejanza si y solo si el polinomio mínimo tiene todas sus raices en K y carece de raices múltiples, o también si, y solo si, todos sus divisores elementales son de grado 1.

**Ejercicio 6.17.** 1. Encuentra la forma normal de Smith de la matriz

$$\begin{pmatrix} x & x^2+1 \\ x-1 & 2x+1 \end{pmatrix}$$

con coeficientes en $\mathbb{Q}[x]$, así como las matrices de paso para alcanzar dicha forma normal. ¿Es $\mathbb{Q}[x]^2/\langle (x, x-1), (x^2+1, 2x+1)\rangle$ cíclico? (razona la respuesta).

2. Sea $M$ el $\mathbb{Q}[x]$ módulo asociado al par $(\mathbb{Q}^3, t)$ con $t$ un endomorfismo con matriz asociada a una base arbitraria $B$,

$$A = \begin{pmatrix} 0 & 4 & -6 \\ -1 & 4 & -3 \\ 0 & 0 & 2 \end{pmatrix}.$$

   *a*) Calcula los factores invariantes de $A$. ¿Es $A$ diagonalizable?

   *b*) Escribe las formas canónicas racional, racional primaria y de Jacobson asociadas a esa matriz.

   *c*) Encuentra bases en las que $t$ tenga como matrices asociadas las formas canónicas del apartado anterior.
   (Se puede hacer uso de la siguiente información: $\{v \in \mathbb{Q}^3 \mid (x-2)v = 0\} = \{\lambda(1,2,1) + \mu(0,3,2) \mid \lambda, \mu \in \mathbb{Q}\}$.)

**Ejercicio 6.18.** Sea $T : \mathbb{R}^3 \to \mathbb{R}^3$ la aplicación lineal cuya matriz, respecto de la base usual, es

$$A = \begin{pmatrix} 1 & -2 & 1 \\ -1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix} \in \mathcal{M}_{3\times 3}(\mathbb{R})$$

y sea $M$ el $\mathbb{R}[x]$-módulo dado por $(\mathbb{R}^3, T)$.

1. Encuentra las descomposiciones cíclica y cíclica primaria de $M$.
2. Encuentra las formas canónicas racional, racional primaria y de Jacobson de la matriz $A$, así como las bases respecto de las cuales tiene dichas formas.

**Ejercicio 6.19.** Sea $T : V \to V$ el endomorfismo de $\mathbb{Q}$-espacios vectoriales que, respecto de una base $B = \{e_1, e_2, e_3\}$, tiene por matriz asociada

$$A = \begin{pmatrix} -1 & -1 & 0 \\ 0 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

Calcular las formas canónicas de la matriz $A$ y las bases respecto de las cuales adopta dichas formas.

## 6.13. Formas canónicas usando GAP

### 6.13.1. Forma normal de Smith de la matriz característica de una matriz

Veamos cómo se puede calcular la forma normal de Smith sobre $\mathbb{Q}[x]$. Primero declaramos que $x$ va a ser la variable con la que vamos a trabajar sobre los racionales.

```
gap> x:=Indeterminate(Rationals,"x");;
```

Empezamos definiendo una matriz.

```
gap> m:=[[7,-2,1],[-2,10,-2],[1,-2,7]];
[ [ 7, -2, 1 ], [ -2, 10, -2 ], [ 1, -2, 7 ] ]
```

Para convertir `m` a una matriz de entradas racionales, la multiplicamos por el elemento neutro de $\mathbb{Q}[x]$. Calculamos $x\mathrm{Id} - m$.

```
gap> mat:=x*m^0-m*One(x);
[ [ x-7, 2, -1 ], [ 2, x-10, 2 ], [ -1, 2, x-7 ] ]
```

Para diagonalizar esta matriz mediante operaciones elementales por filas y columnas, usamos el comando `DiagonalizeMat` indicando el dominio en el que vamos a efectuar las operaciones.

```
gap> DiagonalizeMat(PolynomialRing(Rationals,1),mat);
[ [ 1, 0, 0 ], [ 0, x-6, 0 ], [ 0, 0, x^2-18*x+72 ] ]
```

Podemos también calcular la matriz asociada a un polinomio.

```
gap> CompanionMat(x^2-18*x+72);
[ [ 0, -72 ], [ 1, 18 ] ]
```

O el polinomio característico de una matriz.

```
gap> CharacteristicPolynomial(m);
x^3-24*x^2+180*x-432
gap> Factors(last);
[ x-12, x-6, x-6 ]
```

Así como su polinomio mínimo (el £ltimo factor invariante).

```
gap> MinimalPolynomial(Rationals,m);
x^2-18*x+72
```

Si quisiésemos conocer los vectores propios usamos `Eigenvectors`.

```
gap> Eigenvectors(Rationals,m);
[ [ 1, -2, 1 ], [ 1, 0, -1 ], [ 0, 1, 2 ] ]
gap> Eigenvalues(Rationals,m);
[ 12, 6 ]
```

Y también podemos calcular los subespacios propios asociados a la matriz.

```
gap> lsp:=Eigenspaces(Rationals,m);
[ <vector space over Rationals, with 1 generators>, <vector space over Rationals, with
    2 generators> ]
gap> List(lsp,GeneratorsOfVectorSpace);
[ [ [ 1, -2, 1 ] ], [ [ 1, 0, -1 ], [ 0, 1, 2 ] ] ]
```

### 6.13.2. Cálculo de bases y formas canónicas

Como hemos visto, el comando `DiagonalizeMat` se puede usar para calcular los factores invariantes de una matriz. Por desgracia, en GAP no hay un comando que dé como salida las operaciones elementales por filas y columnas requeridas para llegar a la forma normal de Smith sobre un anillo de polinomios, tal y como ocurría con matrices de entradas enteras. Para salvar este obstáculo mostramos un sencillo procedimiento con un par de ejemplos.

Empezamos definiendo una variable

```
gap> x:=Indeterminate(Rationals,"x");;
```

Dada la matriz

```
gap> a:=[[-1,-1,-1],[-2,0,-1],[6,3,4]];
[ [ -1, -1, -1 ], [ -2, 0, -1 ], [ 6, 3, 4 ] ]
```

de la que queremos conocer su formas canónicas y en las bases en las que éstas se alcanzan, empezamos calculando los factores invariantes de su matriz caracter¡stica

```
gap> xima:=x*a^0-a*One(x);
[ [ x+1, 1, 1 ], [ 2, x, 1 ], [ -6, -3, x-4 ] ]
gap> DiagonalizeMat(PolynomialRing(Rationals,1),xima);
[ [ 1, 0, 0 ], [ 0, x-1, 0 ], [ 0, 0, x^2-2*x+1 ] ]
```

Sabemos por tanto qué aspecto tiene la forma canónica racional asociada a `a`. También obtenemos que el polinomio $x^2 - 2x + 1$ es el polinomio mínimo de la matriz `a`, y en consecuencia es el anulador minimal, esto es, $(x^2 - 2x + 1)v = 0$ para todo $v \in \mathbb{Q}^3$. El siguiente divisor elemental es $x - 1$. Necesitamos un elemento que se anule por $x^2 - 2x + 1$ y que no se anule con $x - 1$. Ese elemento nos servirá para definir el trozo de base asociado a la matriz asociada de $x^2 - 2x + 1$.

```
gap> NullspaceIntMat(TransposedMat(a^2-2*a+a^0));
[ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ]
gap> NullspaceIntMat(TransposedMat(a-a^0));
[ [ 1, 0, -2 ], [ 0, 1, -1 ] ]
gap> [1,0,0] in VectorSpace(Rationals,[[ 1, 0, -2 ], [ 0, 1, -1 ] ]
> );
false
```

Así un candidato bueno para empezar es $(0, 0, 1)$, y al tener $x^2 - 2x + 1$ grado dos, utilizamos también la imagen de éste por `a`.

```
gap> u1:=[1,0,0];
[ 1, 0, 0 ]
gap> u2:=a*[1,0,0];
[ -1, -2, 6 ]
```

Para completar la base, es suficiente con encontrar un elemento en $\mathbb{Q}^3$ que se anule por $x-1$ y que no esté en el subespacio generado por `u1` y `u2`. Como el núcleo de `a`-$Id$ está generado por $\{(1, 0, -2), (0, 1, -1)\}$, y sabemos que no puede ser igual al espacio generado por `u1` y `u2`, probamos con cada uno de los elementos de dicho conjunto.

```
gap> [1,0,-2] in VectorSpace(Rationals,[u1,u2]);
false
gap> v1:=[1,0,-2];
[ 1, 0, -2 ]
```

Así la matriz de cambio de base es

```
gap> s:=TransposedMat([v1,u1,u2]);
[ [ 1, 1, -1 ], [ 0, 0, -2 ], [ -2, 0, 6 ] ]
gap> s^(-1)*a*s;
[ [ 1, 0, 0 ], [ 0, 0, -1 ], [ 0, 1, 2 ] ]
gap> Display(last);
[ [   1,   0,   0 ],
  [   0,   0,  -1 ],
  [   0,   1,   2 ] ]
```

Obteniendo así la forma canónica racional, que en este caso también coincide con la racional primaria.

Para obtener la forma de Jordan y una base en la que se alcanze, modificamos ligeramente el proceso multiplicando $u1$ por a $- Id$ en vez de por a.

```
gap> w1:=u1;
[ 1, 0, 0 ]
gap> w2:=(a-a^0)*u1;
[ -2, -2, 6 ]
gap> [1,0,-2] in VectorSpace(Rationals,[w1,w2]);
false
gap> t:=TransposedMat([v1,w1,w2]);
[ [ 1, 1, -2 ], [ 0, 0, -2 ], [ -2, 0, 6 ] ]
gap> t^(-1)*a*t;
[ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 1, 1 ] ]
```

Veamos ahora otro ejemplo en el que las formas canonicas racional y racional primaria no coinciden.

```
gap> a:=[[4,2,-4],[2,3,-3],[3,2,-3]];
[ [ 4, 2, -4 ], [ 2, 3, -3 ], [ 3, 2, -3 ] ]
gap> xima:=x*a^0-a*One(x);
[ [ x-4, -2, 4 ], [ -2, x-3, 3 ], [ -3, -2, x+3 ] ]
gap> DiagonalizeMat(PolynomialRing(Rationals,1),xima);
[ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, x^3-4*x^2+5*x-2 ] ]
gap> Factors(x^3-4*x^2+5*x-2);
[ x-2, x-1, x-1 ]
gap> u1:=[1,0,0];
[ 1, 0, 0 ]
gap> u2:=a*[1,0,0];
[ 4, 2, 3 ]
gap> u3:=a*u2;
[ 8, 5, 7 ]
gap> s:=TransposedMat([u1,u2,u3]);
[ [ 1, 4, 8 ], [ 0, 2, 5 ], [ 0, 3, 7 ] ]
gap> Display(s^(-1)*a*s);
[ [   0,   0,   2 ],
  [   1,   0,  -5 ],
  [   0,   1,   4 ] ]
```

Como $x^3 - 4x^2 + 5x - 2 = (x-1)^2(x-2)$, para calcular la forma canónica racional primaria necesitamos elementos que se anulen por $(x-1)^2$ y $x-2$. +sos los construimos a partir de u1. El primero de ellos nos

serve para construir el trozo de base que da lugar a la matriz compañera de $(x-1)^2$, y el segundo para la matriz asociada a $x-2$ (que es simplemente un 2).

```
gap> u11:=(a-2*a^0)*u1;
[ 2, 2, 3 ]
gap> u12:=(a-a^0)^2*u1;
[ 1, 1, 1 ]
gap> v1:=u11;
[ 2, 2, 3 ]
gap> v2:=a*u11;
[ 0, 1, 1 ]
gap> v3:=u12;
[ 1, 1, 1 ]
gap> t:=TransposedMat([v1,v2,v3]);
[ [ 2, 0, 1 ], [ 2, 1, 1 ], [ 3, 1, 1 ] ]
gap> Display(t^(-1)*a*t);
[ [   0,  -1,   0 ],
  [   1,   2,   0 ],
  [   0,   0,   2 ] ]
```

La forma de Jordan, y una base en que se consigue, se pueden calcular a partir de parte de la información ya obtenida.

```
gap> w1:=u11;
[ 2, 2, 3 ]
gap> w2:=(a-a^0)*w1;
[ -2, -1, -2 ]
gap> w3:=v3;
[ 1, 1, 1 ]
gap> p:=TransposedMat([w1,w2,w3]);
[ [ 2, -2, 1 ], [ 2, -1, 1 ], [ 3, -2, 1 ] ]
gap> Display(p^(-1)*a*p);
[ [  1,  0,  0 ],
  [  1,  1,  0 ],
  [  0,  0,  2 ] ]
```

### 6.13.3. Forma de Jordan a partir del polinomio característico y subespacios propios

Vemos ahora un método alternativo para calcular formas canónicas de Jordan con un ejemplo, sin pasar previamente por la forma canónica racional primaria.

```
gap> x:=Indeterminate(Rationals,"x");
x
gap> m75:=[[1,0,0,0],[0,1,0,0],[-2,-2,0,1],[-2,0,-1,-2]];
[ [ 1, 0, 0, 0 ], [ 0, 1, 0, 0 ], [ -2, -2, 0, 1 ], [ -2, 0, -1, -2 ] ]
gap> CharacteristicPolynomial(m75);
x^4-2*x^2+1
gap> Factors(last);
[ x-1, x-1, x+1, x+1 ]
```

Usamos las siguientes funciones para calcular los valores propios y los vectores propios.

```
gap> Eigenvectors(Rationals,TransposedMat(m75));
[ [ 1, 0, -2, 0 ], [ 0, 1, -3/2, 1/2 ], [ 0, 0, 1, -1 ] ]
gap> Eigenvalues(Rationals,TransposedMat(m75));
[ 1, -1 ]
```

O bien ...

```
gap> Eigenspaces(Rationals,TransposedMat(m75));
[ <vector space over Rationals, with 2 generators>,
  <vector space over Rationals, with 1 generators> ]
gap> List(last,GeneratorsOfVectorSpace);
[ [ [ 1, 0, -2, 0 ], [ 0, 1, -3/2, 1/2 ] ], [ [ 0, 0, 1, -1 ] ] ]
gap> m75*[1,0,-2,0];
[ 1, 0, -2, 0 ]
gap> m75*[0,0,1,-1];
[ 0, 0, -1, 1 ]
```

Como el núcleo de `m75 + Id` tiene dimensión uno frente a la doble multiplicidad de $(x-1)$ en el polinomio característico, tenemos que calcular el núcleo de $(\mathrm{Id}+\mathtt{m75})^2$, y escoger un elemento del núcleo de $(\mathrm{Id}+\mathtt{m75})^2$ que no esté en el núcleo de `m75 + Id`.

```
gap> NullspaceMat(TransposedMat((m75^0+One(x)*m75)^2));
[ [ 0, 0, 1, 0 ], [ 0, 0, 0, 1 ] ]
gap> (m75^0+m75)*[0,0,0,1];
[ 0, 0, 1, -1 ]
```

Tenemos por tanto la base que buscamos en la que la matriz adopta la forma de Jordan.

```
gap> p:=[[ 1, 0, -2, 0 ], [ 0, 1, -3/2, 1/2 ] ,[0,0,0,1],[0,0,1,-1]];
[ [ 1, 0, -2, 0 ], [ 0, 1, -3/2, 1/2 ], [ 0, 0, 0, 1 ], [ 0, 0, 1, -1 ] ]
gap> p:=TransposedMat(p);
[ [ 1, 0, 0, 0 ], [ 0, 1, 0, 0 ], [ -2, -3/2, 0, 1 ], [ 0, 1/2, 1, -1 ] ]
gap> Display(p^-1*m75*p);
[ [   1,   0,   0,   0 ],
  [   0,   1,   0,   0 ],
  [   0,   0,  -1,   0 ],
  [   0,   0,   1,  -1 ] ]
```

## 6.14. Formas Canónicas de Matrices con MATHEMATICA

La determinación de las formas canónicas de matrices bajo semejanza puede hacerse en MATHEMATICA utilizando un paquete externo para el cálculo de la forma normal de Smith pero, alternativamente, puede eludirse el uso de dicho paquete y hacer el cálculo de forma directa como veremos en la segunda parte de esta práctica.

### 6.14.1. Forma normal de Smith de una matriz

Utilizaremos el siguiente paquete

```
<<"c:/PolynomialSmithNormalForm.m"
```

que nos permitirá calcular la forma normal de Smith de una matriz donde los coeficientes son polinomios. Así, si ponemos

```
aa ={{x+1, x^2}, {x-2, x^3}}; MatrixForm[aa]
```

$$\begin{pmatrix} 1+x & x^2 \\ -2+x & x^3 \end{pmatrix}$$

```
PolynomialSmithForm[aa, x] // MatrixForm
```

$$\begin{pmatrix} 1 & 0 \\ 0 & 2x^2+x^4 \end{pmatrix}$$

Además podremos calcular las matrices $P$ y $Q$ tales que $PAQ$ = Forma Normal

```
ExtendedPolynomialSmithForm[aa, x]
```

$$\left\{\left\{\{1,0\},\ \left\{0,2x^2+x^4\right\}\right\},\right.$$
$$\left.\left\{\left\{\left\{\frac{1}{3},-\frac{1}{3}\right\},\ \{2-x,1+x\}\right\},\ \left\{\left\{1,-\frac{x^2}{3}+\frac{x^3}{3}\right\},\ \{0,1\}\right\}\right\}\right\}$$

Podemos mejorar la salida poniendo

```
L = ExtendedPolynomialSmithForm[aa, x]; MatrixForm[L[[1]]]
P = L[[2,1]]; MatrixForm[P]
Q1 = L[[2,2]]; MatrixForm[Q1]
```

$$\begin{pmatrix} 1 & 0 \\ 0 & 2x^2 + x^4 \end{pmatrix}$$

$$\begin{pmatrix} \frac{1}{3} & -\frac{1}{3} \\ 2 - x & 1 + x \end{pmatrix}$$

$$\begin{pmatrix} 1 & -\frac{x^2}{3} + \frac{x^3}{3} \\ 0 & 1 \end{pmatrix}$$

Comprobamos que efectivamente `P.aa.Q1=PolynomialSmithForm[aa]`

```
Simplify[P.aa.Q1] // MatrixForm
```

$$\begin{pmatrix} 1 & 0 \\ 0 & x^2\left(2 + x^2\right) \end{pmatrix}$$

### 6.14.2. Cálculo de Formas Canónicas de Matrices

Vamos a definir una función que calcule la matriz asociada a un polinomio. Para ello utilizaremos las siguientes funciones:

- La función `CoefficientList[f,x]` que crea una lista con los coeficientes del polinomio $f$.

  Ejemplo

```
f=x^4-5x^2+2x+7;
```

```
CoefficientList[f,x]
```

$$\{7, 2, -5, 0, 1\}$$

- La función `Drop[lista,n]` que suprime el elemento que ocupa el lugar $n$ de una lista (si $n$ es negativo empezamos a contar por el final).

  Ejemplo

```
Drop[CoefficientList[f,x],-1]
```

$$\{7, 2, -5, 0\}$$

- La función `Length[lista]` que calcula la longitud de una lista.
  Ejemplo

```
Length[{a,b,c,d}]
```

$$4$$

- La función `Joint[lista1,lista2]` que une dos listas
  y la función `IdentityMatrix[n]` que escribe la matriz identidad $n \times n$.
  Ejemplo

```
Join[IdentityMatrix[2], {{1, 2}}] // MatrixForm
```

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 2 \end{pmatrix}$$

- La función `Transpose[matrix]` que calcula la transpuesta de una matriz.
  Ejemplo

```
Transpose[Join[IdentityMatrix[2],{{1, 2}}]] // MatrixForm
```

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

Podemos ahora definir una función `MatrizAsociada[f]` que calcule la matriz asociada a un polinomio. Ponemos

```
MatrizAsociada[f_}, x_}] := Transpose[
  Join[
    Transpose[Join[Table[0,
      {i, (Length[CoefficientList[f, x]]-2)}]},
      IdentityMatrix[Length[CoefficientList[f,x]]-2]]],
    {-1 Drop[CoefficientList[f,x],-1]}]]
```

Ejemplo

```
MatrizAsociada[x^3+2, x] // MatrixForm
```

$$\begin{pmatrix} 0 & 0 & -2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Definimos a continuación una función que calcule la matriz suma directa de una lista de matrices.

```
Matrizvarmat[{m1_, m2_}] :=
  Join[Table[Join[m1[[i]],
    Table[0, {j, Length[m2]}]], {i, Length[m1]}],
    Table[Join[Table[0, {j, Length[m1]}],
    m2[[i]]], {i, Length[m2]}]]
Matrizvarmat[{m1_, m2_, m3__}] :=
  Join[
    Table[Join[m1[[i]],
    Table[0, {j, Length[Matrizvarmat[{m2, m3}]]}]],
      {i, {Length[m1]}],
    Table[Join[
      Table[0, {j, Length[m1]}], Matrizvarmat[{m2, m3}][[i]]],
      {i, Length[Matrizvarmat[{m2, m3}]]}]]
```

Ejemplo

```
Matrizvarmat[{{{0, 0, -2}, {1, 0, 0}, {0, 1, 0}},
   {{0 ,0, -2}, {1, 0, 0}, {0, 1, 0}}, {{1, 0}, {0, 1}}}] //
 MatrixForm
```

$$\begin{pmatrix} 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

### 6.14.3. Forma canónica racional

Para el cálculo de la forma canónica racional de una matriz sabemos que tenemos que calcular la forma normal de su matriz característica y luego escribir la suma directa de las matrices asociadas a los factores invariantes. Procedemos con un ejemplo.
Sea

```
A={{-1, 3, 0}, {0, 1, 0}, {0, 2, -1}}; MatrixForm[A]
```

$$\begin{pmatrix} -1 & 3 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & -1 \end{pmatrix}$$

Calculamos la matriz característica

```
B = IdentityMatrix[3] x - A; MatrixForm[B]
```

$$\begin{pmatrix} 1+x & -3 & 0 \\ 0 & -1+x & 0 \\ 0 & -2 & 1+x \end{pmatrix}$$

y calculamos su forma normal

```
B1 = ExtendedPolynomialSmithForm[B, x][[1]]; MatrixForm[B1]
P = ExtendedPolynomialSmithForm[B, x][[2,1]];
Inverse[P] // MatrixForm
```

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1+x & 0 \\ 0 & 0 & -1+x^2 \end{pmatrix}$$

$$\begin{pmatrix} -3 & 0 & 0 \\ -1+x & -\frac{1}{3}+\frac{x}{3} & \frac{1}{2} \\ -2 & -\frac{2}{3} & 0 \end{pmatrix}$$

Por tanto los factores invariantes son

```
d1 := x+1; d2 := x^2-1
```

Entones para calcular la forma canónica racional ponemos:

```
FCR = Matrizvarmat[{MatrizAsociada[d1, x],
      MatrizAsociada[d2, x]}] // MatrixForm
```

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

**Bases para la forma canónica racional**

Seguimos con el ejemplo de arriba. Entonces sabemos que, en este caso, la imagen (donde la acción de x es la imagen por el endomorfismo) de la segunda columna de la inversa de la matriz P da las coordenadas del primer vector de la base mientras que la imagen de la tercera columna y su imagen por el endomorfismos dan los otros dos vectores de la base. Entones, poniendo

```
w1 = Transpose[Inverse[P]][[2]]
w2 = Transpose[Inverse[P]][[3]]
```

$$\left\{0, -\frac{1}{3} + \frac{x}{3}, -\frac{2}{3}\right\}$$

$$\left\{0, \frac{1}{2}, 0\right\}$$

y si

```
T[v_] := A.v
```

tenemos que los tres vectores de la base son

```
v1 = -1/3{0, 1, 0} + 1/3T[{0, 1, 0}] - 2/3{0, 0, 1}
v2 = 1/2{0, 1, 0}
v3 = A.v2
```

$$\{1, 0, 0\}$$

$$\left\{0, \frac{1}{2}, 0\right\}$$

$$\left\{\frac{3}{2}, \frac{1}{2}, 1\right\}$$

Observemos que, ciertamente, $x + 1$ anula a $v1$ y que $x^2 - 1$ anula a $v2$ pues

```
A.v1 + v1
A.A.v2 - v2
```

$$\{0,\ 0,\ 0\}$$

$$\{0,\ 0,\ 0\}$$

Si ponemos

```
Bfcr = {v1, v2, v3}
```

$$\left\{\{1,\ 0,\ 0\},\ \left\{0,\ \tfrac{1}{2},\ 0\right\},\ \left\{\tfrac{3}{2},\ \tfrac{1}{2},\ 1\right\}\right\}$$

y tomamos

```
R = Transpose[Bfcr]; MatrixForm[R]
```

$$\begin{pmatrix} 1 & 0 & \frac{3}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix}$$

entonces tenemos que

```
Inverse[R].A.R // MatrixForm
```

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

que es la forma canónica racional de la matriz dada.

### 6.14.4. Forma canónica racional primaria

Sabemos que la forma canónica racional primaria se calcula a partir de los divisores elementales los cuales se obtienen al factorizar en primos los factores invariantes. Seguimos con el ejemplo anterior y factorizamos entonces los factores invariantes:

```
Factor[x^2-1]
```

$$(-1+x)\,(1+x)$$

Nombramos los divisores elementales

```
p1 = d1
p2 = d2/(-1+x) // Simplify
p3 = d2/(1+x) // Simplify
```

$$1+x$$

$$1+x$$

$$-1+x$$

y, como sabemos, la forma canónica racional primaria se obtiene tomando la suma directa de las matrices asociadas a los divisores elementales. Ponemos entonces:

```
FcrP} =
  Matrizvarmat[{MatrizAsociada[p1, x], MatrizAsociada[p2, x],
    MatrizAsociada[p3, x]}] // MatrixForm
```

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

**Ejercicio:** Sea $T : \mathbb{Q}^5 \longrightarrow \mathbb{Q}^5$la aplicación lineal cuya matriz asociada respecto de la base usual es la matriz $A$ siguiente. Calcular:

1. La forma canónica racional del endomorfismo.
2. Elementos del $\mathbb{Q}$[x]-módulo correspondiente cuyos anuladores sean los factores invariantes. Comprobar el resultado.
3. La base para la forma canónica racional y la matriz del cambio $R$. Comprobar que $R^{-1}AR$ = FCR.
4. Divisores elementales y la forma canónica racional primaria

```
A={{1, -3, -15, -30, -42}, {-3, -5, -15, -24, -12},
   {-3, 7, 33, 66, 78}, {3, -3, -15, -32, -42},
   {-1, 0, 0, 1, 3}};
```

**Ejercicio:** Seguir el método teórico para establecer el proceso que permita calcular las bases en la forma canónica racional primaria.

**Ejercicio:** Escribir una función que devuelva el bloque de Jacobson-Jordan de una potencia de un polinomio irreducible en $\mathbb{Q}$. A partir de ésta, establecer el proceso que permita calcular la forma canónica de Jacobson-Jordan de una matriz así como la base respecto de la cual adopta dicha forma canónica.

### 6.14.5. Cálculo de formas canónicas sin uso de paquetes externos

Como en el caso de grupos abelianos, sabemos que el máximo común divisor de los menores de orden $i$ de una matriz con entradas en un anillo de polinomios con coeficientes en un cuerpo (dominio euclídeo) es el mismo que el de cualquier matriz equivalente a ella. Por tanto, pensando en la forma normal de la matriz característica de una matriz dada, tenemos que el primer factor invariante es el máximo común divisor de los menores de orden 1 y, en general, el $i$-ésimo factor invariante es el cociente del máximo común divisor de los menores de orden $i$ por el de los menores de orden $i-1$. Este es el hecho fundamental que usamos de nuevo para definir las siguientes funciones.

```
mcdmenorespol[a_] := With[{n=Min[Dimensions[a]]},
  Table[PolynomialGCD@@Flatten[Minors[a,i]], {i, 1, n}]]
```

```
factoresinvariantespol[a_] := Module[{men, n},
  men := mcdmenorespol[a];
  n := Length[men];
  Join[{First[men]}, Table[Simplify[men[[i]]/men[[i-1]]],
    {i, 2, n}]]
]
```

**Ejemplo:** Si consideramos la matriz

```
a = {{-1, -1, -1}, {-2, 0, -1}, {6, 3, 4}}; MatrixForm[a]
```

$$\begin{pmatrix} -1 & -1 & -1 \\ -2 & 0 & -1 \\ 6 & 3 & 4 \end{pmatrix}$$

y calculamos su matriz característica

```
m := x IdentityMatrix[3] - a; MatrixForm[m]
```

$$\begin{pmatrix} 1+x & 1 & 1 \\ 2 & x & 1 \\ -6 & -3 & -4+x \end{pmatrix}$$

tenemos que sus factores invariantes los calculamos poniendo

```
factoresinvariantespol[m]
```

$$\left\{1,\ -1+x,\ (-1+x)^2\right\}$$

y poniendo

```
formanormalSmithpol[a_] :=
  DiagonalMatrix[factoresinvariantespol[a]]
```

tenemos que la forma normal de la la matriz característica de la matriz dada es

```
MatrixForm[formanormalSmithpol[m]]
```

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1+x & 0 \\ 0 & 0 & (-1+x)^2 \end{pmatrix}$$

La forma canónica racional se escribe entonces directamente como la suma directa de las matrices asociadas a los factores invariantes. Así si ponemos

```
d1 := -1+x
d2 := (-1+x)^2
```

obtenemos dicha forma canónica racional utilizando la función arriba definida

```
FCR = Matrizvarmat[{MatrizAsociada[d1, x],
  MatrizAsociada[d2, x]}] // MatrixForm
```

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$$

Para calcular la base respecto de la cual la matriz adopta dicha forma procedemos aquí de forma análoga a como se actúa para tal fin en la práctica hecha con GAP. Calculamos entonces una base del subespacio anulado por $x - 1$ poniendo

```
V = NullSpace[a - IdentityMatrix[3]]
```

```
{{−1, 0, 2}, {−1, 2, 0}}
```

Con la función auxiliar

```
pertenece[v_, {vs___}] :=
  MatrixRank[{v, vs}] == MatrixRank[{vs}]
```

buscamos un vector que no pertenezca a dicho subespacio

```
pertenece[{0, 1, -1}, V]
```

```
True
```

```
pertenece[{1, 0, 0}, V]
```

```
False
```

Por tanto el vector

```
u1 = {1, 0, 0}
```

```
{1, 0, 0}
```

y su imagen

```
u2 = a.u1
```

```
{−1, −2, 6}
```

forman una base del subespacio correspondiente al módulo cíclico de anulador $x^2 - 2x + 1$. Para completar la base es suficiente encontrar un vector que no esté en ese subespacio y que se anule por $x - 1$. Entonces, como

```
pertenece[{1, 0, -2}, {u1, u2}]
```

```
False
```

el vector

```
v1 = {1, 0, -2}
```

$$\{1, 0, -2\}$$

nos sirve así que {u1, u2, v1} es la base buscada. Notemos que si ponemos

```
s = Transpose[{v1, u1, u2}]; MatrixForm[s]
```

$$\begin{pmatrix} 1 & 1 & -1 \\ 0 & 0 & -2 \\ -2 & 0 & 6 \end{pmatrix}$$

entonces

```
Inverse[s].a.s // MatrixForm
```

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$$

que es la forma canónica racional que ya habíamos calculado arriba.

**Ejercicio:** Utilizar este método para calcular la forma canónica racional primaria y de Jacobson-Jordan.

**Como ejercicio final se propone encontrar solución a los ejercicios propuestos en la Relación 5 que puedan ser resueltos utilizando las funciones definidas en esta práctica.**

# Bibliografía


[1] J. A. Beachy and W. D. Blair, *Abstract Algebra*, Waveland Press 1996

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press 1966

[3] L. Childs, *A Concrete Introduction to Higher Algebra*, Springer 1979

[4] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer 1978

[5] P. M. Cohn, *Classic Algebra*, Wiley and sons 2000

[6] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Prentice-Hall 1991

[7] J. A. Gallian, *Contemporary Abstract Algebra* 5th edition, Houghton Mifflin 2002

[8] D. E. Knuth, *The Art of Computer Programming, vol. 2: Seminumerical Algorithms* 3rd edition, Addison-Wesley 1998

[9] S. Lang, *Algebra* 3rd edition, Addison-Wesley 1993

[10] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory Of Numbers*, Wiley 1991

[11] N. Jacobson, *Basic Algebra I*, Freeman 1974

[12] S. Lang, *Algebra*, Aguilar 1971

[13] O. Ore, *Number Theory and its History*, Academic Press