Estructuras Algebraicas

Open Course Ware

Javier Jiménez Garrido

Universidad de Cantabria

OPEN COURSE WARE 2023

Para la elaboración de estas notas se ha empleado la *plantilla de LaTeX* 'The Legrand Orange Book' (via http://www.LaTeXTemplates.com) creada por M. Legrand con modificaciones de Vel.

El contenido se ha elaborado tomando como referencia las notas que redactó la profesora Pilar Fernández-Ferreirós Erviti al impartir esta misma asignatura en años anteriores.
Aunque no está demostrado, conjeturo que estas notas contienen errores tipográficos y/o matemáticos de los cuales asumo la absoluta responsabilidad. Empleo estas líneas para disculparme anticipadamente y, a fin de corregirlos en futuras ediciones, agradeceré al lector que me comunique los errores que haya detectado. Si es la primera persona que halla un error que no figura en la lista de actualizaciones, recibirá, como recompensa y si así lo reclama, la solución de un ejercicio de estas notas a su elección.

Impreso por primera vez en marzo de 2021 en Santander.

Impreso por segunda vez en febrero de 2022 en Santander.

Impreso por tercera vez en febrero de 2023 en Santander.

Impreso por cuarta vez en febrero de 2024 en Santander.

Índice general

I Introducción a la teoría de grupos 5

I.1 Grupos: nociones básicas 5

I.2 Subgrupos 8

I.3 Grupos cíclicos y órdenes 13

I.3.1 Grupos cíclicos 13
I.3.2 Orden de un grupo y orden de un elemento 14
I.3.3 Grupos cíclicos finitos 16

I.4 Grupos de permutaciones 19

I.5 Clases Laterales. Subgrupos Normales. Grupo cociente 27

I.5.1 Clases laterales. Teorema de Lagrange 27
I.5.2 Subgrupos normales 31
I.5.3 Grupo cociente 34

I.6 Homomorfismos de grupos 38

I.6.1 Nociones básicas 38
I.6.2 Teoremas de isomorfía 41
I.6.3 Clasificación de grupos de orden p y $2p$. Grupos de orden pequeño 44

II Introducción a la teoría de anillos 53

II.1 Nociones Básicas: Anillos y subanillos 53

II.2 Ideales, anillo cociente y característica 57

II.2.1 Ideales 57
II.2.2 Anillo cociente 59
II.2.3 Característica de un anillo 61

II.3 Homomorfismos de anillos 63

II.3.1 Nociones básicas 63
II.3.2 Teoremas de isomorfía 64

II.3.3 Teorema chino del resto 66
II.4 Dominios y cuerpos 70
II.4.1 Nociones básicas 70
II.4.2 Ideales primos e ideales maximales 73
II.4.3 Cuerpo de fracciones de un dominio 75
II.5 D.F.U., D.I.P. y D.E. 78
II.5.1 Elementos irreducibles y elementos primos de un dominio 78
II.5.2 Dominios de factorización única 81
II.5.3 M.C.D. y M.C.M en dominios de factorización única 82
II.5.4 Dominios de ideales principales 84
II.5.5 Dominios euclídeos 87
II.6 Anillos de polinomios 95
II.6.1 Construcción del anillo de polinomios. Grado de un polinomio 95
II.6.2 Homomorfismo de evaluación. Raíz de un polinomio 98
II.6.3 El dominio $D[x]$ 102
II.6.4 El dominio euclídeo $F[x]$ 105
II.6.5 Polinomios irreducibles y primitivos en $D[x]$ 108
II.6.6 Criterios de irreducibilidad 113

A Apéndice 119
A.1 Número naturales. Principio de inducción 119
A.2 Divisibilidad en $\mathbb{Z}$ 123
A.3 El cuerpo de los números complejos 134

Bibliografía 141
Libros básicos 141
Artículos 141
Libros complementarios 142

Índice alfabético 143

I. Introducción a la teoría de grupos

I.1 Grupos: nociones básicas

Definición I.1.1 Sea G un conjunto no vacío. Toda aplicación $\star$ que a cada par de valores del producto cartesiano $G\times G$ les asigna un valor de G, es decir, $\star : G\times G \to G$, se denomina **operación** o **ley** *(binaria e interna)* en G. Las siguientes propiedades pueden verificarse, o no, por el par $(G,\star)$:

(G.I) **Propiedad asociativa:**
para todos $g,h,f \in G$ se tiene que $g\star(h\star f) = (g\star h)\star f$.

(G.II) **Existencia de elemento neutro:**
existe $e \in G$ tal que para todo $g \in G$ se tiene que $g\star e = e\star g = g$.

(G.III) **Existencia de inverso:**
para todo $g \in G$ existe $\tilde{g} \in G$ tal que: $g\star\tilde{g} = \tilde{g}\star g = e$.

El par $(G,\star)$ se denomina **magma**, y dependiendo de si se satisfacen o no las propiedades anteriores decimos que:

(A) El par $(G,\star)$ es un **semigrupo** si se satisface (G.I).
(B) El par $(G,\star)$ es un **monoide** si se satisface (G.I) y (G.II).
(C) El par $(G,\star)$ es un **grupo** si se satisface (G.I), (G.II) y (G.III).

Si el par $(G,\star)$ es un semigrupo, un monide o un grupo y, adicionalmente, verifica la propiedad:

(G.C) **Propiedad conmutativa**: para todos $g,h \in G$ se tiene que $g\star h = h\star g$.

decimos que $(G,\star)$ es, respectivamente, un semigrupo, un monide o un grupo **abeliano** o **conmutativo**.

Imagen de cabecera: Yayoi Kusama - 'The Souls of Millions of Light Years Away' 2013 (Ver Ejercicio I.3.24)

Ejemplo I.1.2 (1) **Grupos abelianos infinitos**: $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ o $(\mathbb{C},+)$. Para $n\in\mathbb{N}_{\geq 1}$, $(\mathbb{Z}^n,+)$, $(\mathbb{Q}^n,+)$, $(\mathbb{R}^n,+)$ o $(\mathbb{C}^n,+)$. Dados $n,m\in\mathbb{N}_{\geq 1}$, $(\mathrm{Mat}_{n\times m}(\mathbb{Z}),+)$, $(\mathrm{Mat}_{n\times m}(\mathbb{Q}),+)$, $(\mathrm{Mat}_{n\times m}(\mathbb{R}),+)$, $(\mathrm{Mat}_{n\times m}(\mathbb{C}),+)$. El conjunto $\mathrm{Aplic}(\mathbb{R},\mathbb{R})=\{f : f:\mathbb{R}\to\mathbb{R}\}$ de las aplicaciones de $\mathbb{R}$ en $\mathbb{R}$ con la suma, $(\mathrm{Aplic}(\mathbb{R},\mathbb{R}),+)$. Con el producto, por ejemplo, $(\mathbb{Q}\backslash\{0\},\cdot)$, $(\mathbb{R}\backslash\{0\},\cdot)$, $(\mathbb{C}\backslash\{0\},\cdot)$, $(\mathbb{Q}_{>0},\cdot)$ o $(\mathbb{R}_{>0},\cdot)$.

(2) **Grupos abelianos finitos**: Para $k\in\mathbb{N}_{\geq 1}$, $(\mathbb{Z}/k\mathbb{Z},+)$. Para $p\in\mathbb{N}_{\geq 1}$, con p primo, $(\mathbb{Z}/p\mathbb{Z}\backslash\{0\},\cdot)$. Dados $n,m,k\in\mathbb{N}_{\geq 1}$, $(\mathrm{Mat}_{n\times m}(\mathbb{Z}/k\mathbb{Z}),+)$.

(3) **Grupos no abelianos infinitos**: Si $\mathrm{GL}(n,\mathbb{K})$ es el conjunto de matrices $n\times n$ invertibles con coeficientes en $\mathbb{K}$, tenemos que son grupos no abelianos infinitos $(\mathrm{GL}(n,\mathbb{Q}),\cdot)$, $(\mathrm{GL}(n,\mathbb{R}),\cdot)$ y $(\mathrm{GL}(n,\mathbb{C}),\cdot)$ con $n\in\mathbb{N}_{\geq 1}$. El conjunto de las aplicaciones de $\mathbb{R}$ en $\mathbb{R}$ biyectivas con la composición. Las isometrías de $\mathbb{R}^n$ en $\mathbb{R}^n$ con la composición.

(4) **Grupos no abelianos finitos**: Para $p,n\in\mathbb{N}_{\geq 1}$, con p primo el grupo $(\mathrm{GL}(n,\mathbb{Z}/p\mathbb{Z}),\cdot)$.

(5) **No son grupos:** $(\mathbb{N},+)$ es un *monoide*. Son monoides pero no son grupos $(\mathbb{Z}\backslash\{0\},\cdot)$, para $k\in\mathbb{N}_{\geq 1}$ no primo $(\mathbb{Z}/k\mathbb{Z}\backslash\{0\},\cdot)$ y, por ejemplo, $(\mathrm{Mat}_{n\times n}(\mathbb{R})\backslash\{0\},\cdot)$.

Propiedades I.1.3 Sea $(G,\star)$ un grupo. Se cumple que:

(I) el elemento neutro es *único*.

(II) el elemento inverso es *único*.

Demostración. (I) Supongamos que existen dos elementos neutros $e_1,e_2\in G$ que satisfacen la propiedad (G.II), entonces tenemos que:

$$e_1 \overset{\substack{e=e_2,\ g=e_1\\ \text{(G.II)}}}{=} e_1\star e_2 \overset{\substack{e=e_1,\ g=e_2\\ \text{(G.II)}}}{=} e_2.$$

(II) Dado $g\in G$ supongamos que existen dos elementos inversos de g, que denotamos por $\tilde{g}_1,\tilde{g}_2\in G$. Por (G.III), tenemos que $g\star\tilde{g}_1=\tilde{g}_1\star g=e$ y que $g\star\tilde{g}_2=\tilde{g}_2\star g=e$. Por tanto, se cumple que

$$\tilde{g}_2 \overset{\text{(G.II)}}{=} \tilde{g}_2\star e \overset{\text{(G.III)}}{=} \tilde{g}_2\star(g\star\tilde{g}_1) \overset{\text{(G.I)}}{=} (\tilde{g}_2\star g)\star\tilde{g}_1 \overset{\text{(G.III)}}{=} e\star\tilde{g}_1 \overset{\text{(G.II)}}{=} \tilde{g}_1.$$

■

Notación I.1.4 Como es único se representa habitualmente por 1_G, o simplemente, 1 si la operación en G es el producto y por 0_G, o simplemente, 0 si la operación es la suma. Del mismo modo, como es único el inverso de g se representa por por g^{-1} si la operación es el producto y por $-g$ si la operación es la suma. Dado $n\in\mathbb{N}_{\geq 1}=\{1,2,\dots\}$, el resultado de operar un elemento g consigo mismo n veces, lo denotamos por g^n si usamos notación multiplicativa y por ng si usamos notación aditiva. Del mismo modo, el resultado de operar g^{-1} con él mismo n veces se denota por g^{-n} si usamos notación multiplicativa y por $-ng$ si usamos notación aditiva. Finalmente, denotamos por $g^0=1_G$ y $0g=0_G$ en las correspondientes notaciones. En otras palabras, para todo $n\in\mathbb{N}_{\geq 1}$ se tiene que

$$g^n := \overbrace{g\cdot g\cdots g}^{n\text{ factores}}, \qquad g^{-n} := \overbrace{g^{-1}\cdot g^{-1}\cdots g^{-1}}^{n\text{ factores}}, \qquad \textit{(Notación multiplicativa)}$$

$$ng := \overbrace{g+g+\cdots+g}^{n\text{ sumandos}}, \qquad -ng := \overbrace{(-g)+(-g)+\cdots+(-g)}^{n\text{ sumandos}}. \qquad \textit{(Notación aditiva)}$$

Gracias a la propiedad asociativa, esta definición no es ambigua y, para todos $n,m\in\mathbb{Z}$, podemos probar que

$$g^{m+n}=g^ng^m, \qquad (g^n)^m=g^{n\cdot m}, \qquad \textit{(Notación multiplicativa)}$$

$$(m+n)g=ng+mg, \qquad (m(ng))=(nm)g. \qquad \textit{(Notación aditiva)}$$

	Notación multiplicativa $(G,\bullet)$	**Notación aditiva** $(G,+)$
Operación	$g\cdot h$ ó gh	$g+h$
Neutro	1_G ó 1	0_G ó 0
Inverso/opuesto	g^{-1}	$-g$
Operación iterada de un elemento	g^n	ng
Operación iterada de su inverso	g^{-n}	$-ng$

Por simplicidad, de ahora en adelante utilizaremos la **notación multiplicativa** para enunciar y demostrar los resultados generales de teoría de grupos, es decir, consideraremos grupos de la forma $(G,\bullet)$. No obstante, hay que entender que las todas las propiedades, proposiciones, lemas, teoremas y corolarios son ciertos para grupos aditivos $(G,+)$ o de cualquier otro tipo, haciendo los cambios pertinentes en la notación.

Ejercicio I.1.5 Justificar por qué las afirmaciones del Ejemplo I.1.2 son ciertas.

Ejercicio I.1.6 (Enteros módulo n). Dado $n\in\mathbb{N}_{\geq 1}=\{1,2,\dots\}$ se considera el conjunto $\mathbb{Z}/n\mathbb{Z}:=\{0,1,\dots,n-1\}$. Para cada entero $a\in\mathbb{Z}$ el algoritmo de la división de a entre n asocia a a un único elemento de $\mathbb{Z}/n\mathbb{Z}$ (ver Teorema A.2.3). Esta propiedad nos permite definir una suma y un producto en $\mathbb{Z}/n\mathbb{Z}$:

(Suma) Para cada dos elementos $a,b\in\mathbb{Z}/n\mathbb{Z}$ se define su suma en $\mathbb{Z}/n\mathbb{Z}$ como el $r\in\mathbb{Z}/n\mathbb{Z}$ definido mediante la división de $a+b$ entre n, es decir,

$$\text{si } a+b=qn+r \text{ con } 0\leq r<n, \text{ entonces } a+b:=r$$

(Producto) Para cada dos elementos $a,b\in\mathbb{Z}/n\mathbb{Z}$ se define su producto en $\mathbb{Z}/n\mathbb{Z}$ como el $r\in\mathbb{Z}/n\mathbb{Z}$ definido mediante la división de $a\cdot b$ entre n, es decir,

$$\text{si } a\cdot b=qn+r \text{ con } 0\leq r<n, \text{ entonces } a\bullet b:=r$$

Probar que:

(I) $(\mathbb{Z}/n\mathbb{Z},+)$ es un grupo abeliano.

(II) $(\mathbb{Z}/n\mathbb{Z},\bullet)$ es un monoide conmutativo.

Ejercicio I.1.7 (Unidades en $\mathbb{Z}/n\mathbb{Z}$). Sea $n\in\mathbb{N}_{\geq 2}$. Un elemento $a\in\mathbb{Z}/n\mathbb{Z}$, decimos que a **es una unidad de** $\mathbb{Z}/n\mathbb{Z}$ si a tiene inverso para el producto, es decir, si existe $b\in\mathbb{Z}/n\mathbb{Z}$ tal que $a\bullet b=b\bullet a=1$. El conjunto de unidades de $\mathbb{Z}/n\mathbb{Z}$ se denota por

$$U(\mathbb{Z}/n\mathbb{Z}):=\{a\in\mathbb{Z}/n\mathbb{Z}:\ \exists b\in\mathbb{Z}/n\mathbb{Z} \text{ tal que } a\bullet b=b\bullet a=1\}.$$

Probar que:

(I) $(U(\mathbb{Z}/n\mathbb{Z}),\ \bullet)$ es un grupo abeliano.

(II) $U(\mathbb{Z}/n\mathbb{Z})=\{a\in\mathbb{Z}/n\mathbb{Z}:\text{m.c.d.}(a,n)=1\}$ (ver Definición A.2.5).

Ejercicio I.1.8 (Grupo diédrico). El **grupo diédrico** D_n es el grupo de isometrías del plano que dejan invariante un polígono regular de n lados.

(I) Busca información sobre D_3 y descríbelo (lista de elementos y tabla), es decir, el grupo de isometrías del plano que dejan invariante un triángulo equilátero.

(II) Busca información y describe D_4.

(III) ¿Son D_3 y D_4 abelianos?

Ejercicio I.1.9 (Grupo producto). Dados dos grupos $(G,\star)$, $(H,\perp)$, se define una operación sobre el producto cartesiano $G\times H$ del modo siguiente:

$$\begin{aligned} *:(G\times H)\times(G\times H) &\longrightarrow G\times H\\ ((g_1,h_1),(g_2,h_2)) &\longrightarrow (g_1\star g_2, h_1\perp h_2)\end{aligned}$$

Probar que $(G\times H,*)$ es un grupo. Probar que si G y H son abelianos, entonces $G\times H$ también lo es. En el caso de grupos abelianos aditivos a veces se denota al grupo producto por $G\oplus H$. (*Extra: Comprobar que esta construcción se extiende sin problemas para cualquier conjunto finito de grupos*)

Ejercicio I.1.10 Empleando la definición de los Ejercicios I.1.6 y I.1.9 construir la tabla aditiva de los grupos $(\mathbb{Z}/2\mathbb{Z},+)\times(\mathbb{Z}/3\mathbb{Z},+)$ y $(\mathbb{Z}/2\mathbb{Z},+)\times(\mathbb{Z}/4\mathbb{Z},+)$. Comparar las tablas obtenidas con las tablas de $(\mathbb{Z}/6\mathbb{Z},+)$ y $(\mathbb{Z}/8\mathbb{Z},+)$ respectivamente.

Ejercicio I.1.11 Probar que si $a,a_1,a_2\ldots a_n$ son elementos de un grupo $(G,\bullet)$ y $n\in\mathbb{N}_{\geq 1}$ se cumple que: $(a^{-1})^{-1}=a$ y $(a_1a_2\cdots a_n)^{-1}=a_n^{-1}\cdots a_2^{-1}a_1^{-1}$.

I.2 Subgrupos

Definición I.2.1 Sean $(G,\bullet)$ un grupo y $H\subseteq G$ un subconjunto no vacío. Decimos que H es un **subgrupo** de G si al restringir la operación binaria $\bullet$ a H tenemos que $(H,\bullet_{|H\times H})$ es un grupo.

Observación I.2.2 Para todo grupo $(G,\bullet)$ los subconjuntos $\{1_G\}$ y G son siempre subgrupos.

Ejemplo I.2.3 (1) $\mathbb{Z}$ es un subgrupo de $(\mathbb{Q},+)$.
(2) $\mathbb{Q}\backslash\{0\}$ es subgrupo de $(\mathbb{R}\backslash\{0\},\cdot)$.
(3) Dado $n\in\mathbb{N}=\{0,1,2,3\ldots\}$, tenemos que $n\mathbb{Z}=\{na : a\in\mathbb{Z}\}$ es un subgrupo de $(\mathbb{Z},+)$. (ver Ejercicio I.2.17)
(4) Para $n\in\mathbb{N}_{\geq 2}$, $\mathbb{Z}/n\mathbb{Z}=\{0,1,\ldots,n-1\}$ no es un subgrupo de $(\mathbb{Z},+)$. Aunque, como se ha visto en el Ejercicio I.1.6, es posible definir una operación suma en $\mathbb{Z}/n\mathbb{Z}$, la suma módulo n no es la restricción de la suma de $(\mathbb{Z},+)$ a $\mathbb{Z}/n\mathbb{Z}$. Por ejemplo con la suma de $\mathbb{Z}$ tenemos que $1+1=2$ pero con la suma definida en $\mathbb{Z}/2\mathbb{Z}$ tenemos $1+1=0$.
(5) El subconjunto de las matrices simétricas o el subconjunto de las matrices diagonales de tamaño $n\times n$ con coeficientes en $\mathbb{R}$ son subgrupos de $(\mathrm{Mat}_{n\times n}(\mathbb{R}),+)$.

El siguiente resultado nos proporciona un método sencillo para comprobar si un subconjunto no vacío de un grupo es o no es un subgrupo sin necesidad de comprobar directamente todos los axiomas de la definición de grupo.

Proposición I.2.4 — Test de caracterización de subgrupos. Sean $(G,\bullet)$ un grupo y H un subconjunto no vacio de G. Son equivalentes:
(I) H es subgrupo de G.
(II) Para todos $x,y\in H$ se cumple que $x\bullet y^{-1}\in H$.

Demostración. (I) $\Rightarrow$ (II) Supongamos que H es un subgrupo de G, entonces la operación de G restringida a H, $\bullet_{|H\times H}:H\times H\to H$ es una operación interna y $(H,\bullet_{|H\times H})$ satisface (G.I), (G.II) y (G.III). En primer lugar, veamos que $1_G=1_H$. Como $(H,\bullet_{|H\times H})$ y $(G,\bullet)$ son grupos

tenemos que

$$1_G \overset{\text{(G.III) en G}}{=} 1_H \cdot (1_H)^{-1} \overset{\text{(G.II) en H}}{=} (1_H \cdot 1_H) \cdot (1_H)^{-1} \overset{\text{(G.I) en G}}{=} 1_H \cdot (1_H \cdot (1_H)^{-1}) \overset{\text{(G.III) en G}}{=} 1_H \cdot 1_G \overset{\text{(G.II) en G}}{=} 1_H.$$

En consecuencia, se tiene que $1_G = 1_H \in H$. Veamos que se cumple (II). Dados $x, y \in H$, por (G.III) en H, existe $\tilde{y} \in H$ tal que $y \cdot \tilde{y} = \tilde{y} \cdot y = 1_H = 1_G$. Como $y \in H \subseteq G$, por (G.III) en G, existe $y^{-1} \in G$ tal que $y \cdot y^{-1} = y \cdot y^{-1} = 1_G$. Por la unicidad del inverso en G, Propiedad I.1.3.(II) se tiene que $y^{-1} = \tilde{y} \in H$. Finalmente, como $x, y^{-1} \in H$ y como $\cdot_{|H \times H} : H \times H \to H$, concluimos que $x \cdot y^{-1} \in H$.

(II) $\Rightarrow$ (I) Supongamos que para todos $x, y \in H$ se cumple que $x \cdot y^{-1} \in H$. En primer lugar vemos que se cumplen las siguientes propiedades:

(a) $1_G \in H$.
(b) Si $x \in H$, entonces $x^{-1} \in H$.
(c) Si $x, y \in H$, entonces $x \cdot y \in H$.

(a) Como H es no vacío, existe $h \in H$. Por (II), como $h, h \in H$, tenemos que $h \cdot h^{-1} \in H$. Por (G.III) en $(G, \cdot)$, se cumple que $h \cdot h^{-1} = 1_G$, luego $1_G \in H$.
(b) Dado $x \in H$, por (a), se tiene que $1_G, x \in H$. Por tanto, por (II), tenemos que $1_G \cdot x^{-1} \in H$. Por (G.II) en $(G, \cdot)$, se cumple que $1_G \cdot x^{-1} = x^{-1}$, luego $x^{-1} \in H$.
(c) Dados $x, y \in H$, por (b), se cumple que $y^{-1} \in H$. Consecuentemente, por (II), como $x, y^{-1} \in H$, tenemos que $x \cdot (y^{-1})^{-1} \in H$. Por el Ejercicio I.1.11, tenemos que $y = (y^{-1})^{-1}$ y concluimos que $x \cdot y \in H$.

Por hipótesis, sabemos que que $H \neq \emptyset$. Por (c) tenemos que $\cdot_{|H \times H}$ es una operación binaria interna en H, es decir, $\cdot_{|H \times H} : H \times H \to H$. Como se cumple (G.I) en G, también se cumple en $(H, \cdot_{|H \times H})$. Dado que 1_G es el elemento neutro de G y que, por (a), $1_G \in H$ tenemos que se cumple (G.II) en $(H, \cdot_{|H \times H})$. Finalmente, como se cumple (G.III) en G y que, por (b), si $x \in H$, entonces $x^{-1} \in H$, deducimos que se cumple (G.III) en $(H, \cdot_{|H \times H})$ y concluimos que $(H, \cdot_{|H \times H})$ es un grupo. ■

Observación I.2.5 Como consecuencia de la prueba del test de caracterización tenemos que si H es un subgrupo de $(G, \cdot)$, entonces:

(a) $1_G \in H$.
(b) Si $x \in H$, entonces $x^{-1} \in H$.
(c) Si $x, y \in H$, entonces $x \cdot y \in H$.

Recíprocamente, si H es un subconjunto de G y se verifican las tres condiciones anteriores, entonces H es un subgrupo de G. Para comprobar esto, basta observar que: como $1_G \in H$, tenemos que H es no vacío y que dados $x, y \in H$, por (b), $y^{-1} \in H$ y, por (c), como $x, y^{-1} \in H$ tenemos que $x \cdot y^{-1} \in H$. En consecuencia, si H satisface las condiciones (a), (b) y (c) por el test de caracterización de subgrupos, Proposición I.2.4, concluimos que H es un subgrupo de G.

Proposición I.2.6 Sea $(G, \cdot)$ un grupo y $\{H_i\}_{i \in I}$ una familia de subgrupos. Se cumple que:

$$H = \cap_{i \in I} H_i \text{ es un subgrupo de } G.$$

Demostración. Como para todo $i \in I$ se cumple que $1_G \in H_i$, tenemos que $1_G \in H$ luego H es no vacío. Dados $x, y \in H = \cap_{i \in I} H_i$, para todo $i \in I$ tenemos que $x, y \in H_i$. Como para todo $i \in I$ el subconjunto H_i es subgrupo de G, por el test de caracterización de subgrupos, Proposición I.2.4, para todo $i \in I$ se cumple que $x \cdot y^{-1} \in H_i$. En consecuencia, deducimos que $x \cdot y^{-1} \in \cap_{i \in I} H_i = H$. Finalmente, de nuevo por el test de caracterización de subgrupos, Proposición I.2.4, concluimos que H es subgrupo de G. ■

Observación I.2.7 En general, la unión de subgrupos no es un subgrupo.

Ejemplo I.2.8 Por el Ejercicio I.2.17, sabemos que $2\mathbb{Z} = \{2a : a \in \mathbb{Z}\}$ y $3\mathbb{Z} = \{3a : a \in \mathbb{Z}\}$ son un subgrupos de $(\mathbb{Z}, +)$. Veamos que $A = 2\mathbb{Z} \cup 3\mathbb{Z}$ no es un subgrupo. Tenemos que $2 \in 2\mathbb{Z}$ y que $3 \in 3\mathbb{Z}$ pero $5 = 2+3 \notin A$, luego la suma restringida a A no es una operación interna y, en consecuencia, A no es un subgrupo.

Definición I.2.9 Sea $(G, \bullet)$ un grupo y X un subconjunto de G. Llamamos **subgrupo generado por** X a la intersección de todos los subgrupos G que contienen a X, lo denotamos por $< X >$, es decir,

$$< X > \quad := \bigcap_{\substack{X \subseteq H \\ H \text{ subgrupo de } G}} H.$$

Observación I.2.10 Por la Proposición I.2.6, sabemos que $< X >$ es un subgrupo. Además, es el menor (para la relación de contenido) subgrupo de G que contiene a X, es decir, si H es un subgrupo y $X \subseteq H$, entonces se tiene que $< X > \subseteq H$.

Proposición I.2.11 Sean $(G, \bullet)$ un grupo y X un subconjunto no vacío de G. Entonces $< X >$ está formado por los productos de los elementos de X y sus inversos, es decir,

$$< X >= \left\{ x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r} : r \in \mathbb{N}_{\geq 1}, x_i \in X, e_i \in \{1, -1\} \right\}.$$

Demostración. Denotamos por $A := \left\{ x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r} : r \in \mathbb{N}_{\geq 1}, x_i \in X, e_i \in \{1, -1\} \right\}$.

(a) Veamos que $< X > \subseteq A$. Para ello veamos que A es un subgrupo que contiene a X.

(a.1) Observamos que todo elemento x de X, tiene la forma de un elemento de A para $r = 1$ y $e_1 = 1$, luego $x \in A$. En consecuencia, $X \subseteq A$ y, como $X \neq \emptyset$, también $A \neq \emptyset$.

(a.2) Dados $x, y \in A$, tenemos que existen $r, s \in \mathbb{N}_{\geq 1}$, $x_i, y_j \in X$ y $e_i, d_j \in \{1, -1\}$ para todo $i \in \{1, \ldots, r\}$ y todo $j \in \{1, \ldots, s\}$, tales que

$$x = x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r} \qquad y = y_1^{d_1} y_2^{d_2} \cdots y_s^{d_s}.$$

Por el Ejercicio I.1.11, se tiene que $y^{-1} = (y_1^{d_1} y_2^{d_2} \cdots y_s^{d_s})^{-1} = y_s^{-d_s} \cdots y_2^{-d_2} y_1^{-d_1}$ entonces $xy^{-1} = x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r} y_s^{-d_s} \cdots y_2^{-d_2} y_1^{-d_1}$ tiene la forma requerida, luego $xy^{-1} \in A$. Por el test de caracterización de subgrupos, Proposición I.2.4, A es un subgrupo.

Como A es un subgrupo que contiene a X, por la Observación I.2.10, $< X > \subseteq A$.

(b) Veamos que $A \subseteq < X >$. Dado $x \in A$, $x = x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r}$ con $r \in \mathbb{N}_{\geq 1}$, $x_i \in X$, $e_i \in \{1, -1\}$. Como $X \subseteq < X >$ y como $< X >$ es subgrupo, tenemos que $x_i^{-1} \in < X >$, luego para todo índice $i \in \{1, \ldots, r\}$ tenemos que $x_i^{e_i} \in < X >$. De nuevo como $< X >$ es subgrupo, $x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r} \in < X >$, es decir, $x \in < X >$ y concluimos que $A \subseteq < X >$. ■

Notación I.2.12 Cuando el conjunto X está formado por un número finito de elementos $X = \{x_1, x_2, \ldots, x_n\}$, por brevedad, denotaremos por $< x_1, x_2, \ldots, x_n >$ al subgrupo generado por X en lugar de $< \{x_1, x_2, \ldots, x_n\} >$, es decir, eliminando las llaves de conjunto.

Ejemplo I.2.13 (1) En $(\mathbb{Z}, +)$, teniendo en cuenta que la notación es aditiva (ver Notación I.1.4), tenemos que

$$< 1 >=< \{1\} >= \left\{ \overbrace{\pm 1 \pm 1 \cdots \pm 1}^{\text{r sumandos}} : r \in \mathbb{N}_{\geq 1} \right\}.$$

En consecuencia, deducimos que $\mathbb{Z} =< 1 >$. En general, para todo $k \in \mathbb{Z}$ se tiene que

$$< k >=< \{k\} >= \left\{ \overbrace{\pm k \pm k \cdots \pm k}^{\text{r sumandos}} : r \in \mathbb{N}_{\geq 1} \right\} = \left\{ ka : a \in \mathbb{Z} \right\} = k\mathbb{Z}.$$

(2) En $(\mathbb{Z},+)$ se tiene que $<2,3>=<\{2,3\}>=\mathbb{Z}$.
(3) En $(\mathbb{Q},+)$ tenemos que $<1/3>$ es un subgrupo distinto del total que contiene a $\mathbb{Z}$.

Observación I.2.14 Podemos probar, empleando la Proposición I.2.11 que si $(G,\cdot)$ y $a\in G$ entonces $<a>=\{a^n : n\in\mathbb{Z}\}$.

Observación I.2.15 Podemos probar que si S_1 y S_2 son subgrupos el menor subgrupo de $(G,\cdot)$ que contiene a ambos es $<S_1\cup S_2>$.

Observación I.2.16 En un $\mathbb{K}-$espacio vectorial V dado $E\subseteq V$, en ocasiones $<E>$ denota el subespacio vectorial generado por E. Sin embargo, en este curso reservaremos la notación $<E>$ para el subgrupo generado por E y y, si por algún casual, queremos considerar el subespacio vectorial generado por E en el $\mathbb{K}-$espacio vectorial V escribiremos $\mathbb{K}<E>$. Por ejemplo en $\mathbb{R}^2$, como $\mathbb{R}-$espacio vectorial, el subespacio generado por $\{(1,0)\}$ sería

$$\mathbb{R}<\{(1,0)\}>=\{(\alpha,0) : \alpha\in\mathbb{R}\}=\mathbb{R}\times\{0\}.$$

Sin embargo, en el grupo producto $(\mathbb{R}^2,+)$, el subgrupo generado por $\{(1,0)\}$ sería

$$<\{(1,0)\}>=\{(m,0) : m\in\mathbb{Z}\}=\mathbb{Z}\times\{0\}.$$

Ejercicio I.2.17 (Subgrupos de $\mathbb{Z}$). Sea H un subconjunto no vacío de $\mathbb{Z}$. Probar que son equivalentes:
(I) H es subgrupo de $(\mathbb{Z},+)$.
(II) Existe $n\in\mathbb{N}$ tal que $H=n\mathbb{Z}=\{na : a\in\mathbb{Z}\}$.

Ejercicio I.2.18 Determinar si S y/o T son o no subgrupos en cada caso.
(I) En $(\mathbb{C},+)$ consideramos $S=\mathbb{R}$ y $T=\{a+bi\in\mathbb{C} : a\leq 2\}$.
(II) En $(\mathbb{Q}\backslash\{0\},\cdot)$ consideramos $S=\mathbb{Z}\backslash\{0\}$ y $T=\{x\in\mathbb{Q} : x>0\}$.

Ejercicio I.2.19 Probar que si $a_1,a_2,\ldots a_n$ son números enteros, d es su m.c.d. y m su m.c.m. (Ver Definiciones A.2.5 y A.2.6), se cumple que

$$\langle a_1\rangle\cap\langle a_2\rangle\cap\cdots\cap\langle a_n\rangle=\langle m\rangle \quad \text{y} \quad \langle a_1,a_2,\ldots,a_n\rangle=\langle d\rangle.$$

Ejercicio I.2.20 Para cada uno de los siguientes grupos determinar todos los elementos que forman los subgrupos S y T:
(I) En $(\mathbb{Z},+)$, $S=\langle 27,15,6,51\rangle$, $T=\langle 18,30\rangle\cap\langle 6,15\rangle$.
(II) En $(\mathbb{Z}/3\mathbb{Z},+)\times(\mathbb{Z}/8\mathbb{Z},+)$ (ver Ejercicio I.1.9), $S=\langle(2,4)\rangle$ y $T=\langle(1,1)\rangle$.

Ejercicio I.2.21 (Centro de un grupo). Dado un grupo $(G,\cdot)$, denominamos **centro de** G al subconjunto

$$Z(G):=\{a\in G : \forall b\in G \;\; ab=ba\}.$$

Demostrar que $Z(G)$ es un subgrupo de G. ¿Si G es finito como se puede localizar $Z(G)$ en la tabla de G? Calcular $Z(D_3)$ y $Z(D_4)$.

Ejercicio I.2.22 (Cuaterniones de Hamilton). Un cuaternión es un elemento de $\mathbb{R}^4$ en lugar de la notación (a_1,a_2,a_3,a_4) empleamos para denotarlo una expresión de la forma $a_1+a_2\mathbf{i}+a_3\mathbf{j}+a_4\mathbf{k}$ donde $a_1,a_2,a_3,a_4\in\mathbb{R}$. El conjunto de todas las expresiones de este tipo se denota por $\mathbb{H}:=\{a_1+a_2\mathbf{i}+a_3\mathbf{j}+a_4\mathbf{k} : a_1,a_2,a_3,a_4\in\mathbb{R}\}$. Podemos definir la suma y el producto de dos de estas expresiones del siguiente modo:

$$\begin{aligned} a+b :=& (a_1+a_2\mathbf{i}+a_3\mathbf{j}+a_4\mathbf{k})+(b_1+b_2\mathbf{i}+b_3\mathbf{j}+b_4\mathbf{k}) \\ =& (a_1+b_1)+(a_2+b_2)\mathbf{i}+(a_3+b_3)\mathbf{j}+(a_4+b_4)\mathbf{k}. \end{aligned}$$

$$\begin{aligned} a\cdot b :=& (a_1+a_2\mathbf{i}+a_3\mathbf{j}+a_4\mathbf{k})(b_1+b_2\mathbf{i}+b_3\mathbf{j}+b_4\mathbf{k}) \\ =& (a_1b_1-a_2b_2-a_3b_3-a_4b_4)+(a_1b_2+a_2b_1+a_3b_4-a_4b_3)\mathbf{i} \\ &+(a_1b_3-a_2b_4+a_3b_1+a_4b_2)\mathbf{j}+(a_1b_4+a_2b_3-a_3b_2+a_4b_1)\mathbf{k}. \end{aligned}$$

Se pide:

(I) Demostrar que $(\mathbb{H},+)$ y $(\mathbb{H}\backslash\{0\},\cdot)$ son grupos. ¿Son abelianos?

(II) Probar que $i^2=j^2=k^2=-1=ijk$.

(III) Probar que el conjunto $Q_8=\{\pm1,\pm i,\pm j,\pm k\}$ es un subgrupo de $(\mathbb{H}\backslash\{0\},\cdot)$ no abeliano, que se denomina **grupo de los cuaterniones**.

(IV) Obtener la tabla multiplicativa de Q_8 y obtener $Z(Q_8)$ (Ver Ejercicio I.2.21).

Ejercicio I.2.23 (Normalizador de un conjunto). Dado un grupo $(G,\cdot)$ y sea A un subconjunto de G no vacío, denominamos **normalizador de** A al subconjunto

$$N(A):=\{x\in G : xA=Ax\},$$

donde $xA=\{xa : a\in A\}$ y $Ax=\{ax : a\in A\}$. Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(I) $N(A)$ es un subgrupo de G.

(II) $N(\{1_G\})=G$

(III) Si G es abeliano, entonces para todo subconjunto $A\subseteq G$ con $A\neq\emptyset$ se cumple que $N(A)=G$.

(IV) En $(\mathbb{Z},+)$ tenemos que $N(2\mathbb{Z})=\mathbb{Z}$.

(V) En D_3 si R es el conjunto formado por la identidad y las dos rotaciones entonces $N(R)=D_3$.

(VI) En D_3 si S es el conjunto formado por la identidad y una de las simetrías entonces $N(S)=S$.

(VII) $N(G)=G$ si y solo si G es abeliano.

(VIII) Siempre se cumple que $N(G)=Z(G)$.

(IX) Siempre se cumple que $N(Z(G))=G$.

(X) Siempre se cumple que $Z(N(G))=Z(G)$.

I.3 Grupos cíclicos y órdenes

I.3.1 Grupos cíclicos

Definición I.3.1 Un grupo $(G,\bullet)$ es **cíclico** si está generado por un solo elemento, es decir, G es cíclico si y solo si existe $a \in G$ tal que $G =< a >$.

Ejemplos I.3.2 (1) De acuerdo con el Ejemplo I.2.13.(1), tenemos que $\mathbb{Z} =< 1 >$, luego $(\mathbb{Z},+)$ es cíclico.
(2) $(\mathbb{Q},+)$ no es cíclico, basta observar que para todo $q \in \mathbb{Q}$, $q \neq 0$, $q/2 \in \mathbb{Q}$ pero $q/2 \notin < q >$.
(3) Para todo $n \in \mathbb{N}_{\geq 1}$, tenemos que $\mathbb{Z}/n\mathbb{Z}$ es un grupo cíclico porque $\mathbb{Z}/n\mathbb{Z} =< 1 >$.
(4) El conjunto de las raíces $n-$ésimas de la unidad $R_n = \{e^{2k\pi i/n} : 0 \leq k \leq n-1\}$, es un grupo cíclico con el producto.

Teorema I.3.3 Todo grupo cíclico es abeliano.

Demostración. Dado un grupo cíclico $(G,\bullet)$ y $x,y \in G$, existen $a \in G$ tal que $G =< a >$ y existen $j,k \in \mathbb{Z}$ tales que $x = a^j$ e $y = a^k$. Empleando las propiedades de la Notación I.1.4 y la conmutatividad de la suma en $\mathbb{Z}$ vemos que

$$xy = a^j a^k = a^{j+k} = a^{k+j} = a^k a^j = yx.$$

En consecuencia, G es abeliano. ■

Observación I.3.4 El recíproco no es cierto (Ver Ejercicio I.3.19).

Ejemplo I.3.5 Hemos probado que los grupos D_3 y D_4 (Ejercicio I.1.8) no son abelianos, por tanto, por el Teorema I.3.3 tampoco son cíclicos.

Proposición I.3.6 Todo subgrupo de un grupo cíclico es cíclico.

Demostración. Dado un grupo cíclico $(G,\bullet)$ y H un subgrupo de G, existe $a \in G$ tal que $G =< a >$. Distinguimos dos casos:

(a) Si $H = \{1_G\}$, tenemos que $H =< 1_G >$ y, por tanto, es cíclico.

(b) Si $H \neq \{1_G\}$, existe $x \in H$, $x \neq 1_G$. Como $G =< a >$, existe $m \in \mathbb{Z}$ con $m \neq 0$ tal que $x = a^m$. Como H es subgrupo, $x^{-1} = a^{-m} \in H$. En resumen, podemos suponer que existe $k \in \mathbb{N}_{\geq 1}$ tal que $a^k \in H$.
Consideramos $A := \{k \in \mathbb{N}_{\geq 1} : a^k \in H\}$, como $A \neq \emptyset$ y $A \subseteq \mathbb{N}_{\geq 1}$, por el Principio de Buena Ordenación (Teorema A.1.2) existe $d = \text{mín}(A)$. Veamos que $H =< a^d >$.

$(\supseteq)$ Como H es subgrupo, $< a^d > \subseteq H$ porque $a^d \in H$.

$(\subseteq)$ Dado $y \in H$, como $G =< a >$, existe $n \in \mathbb{Z}$ tal que $y = a^n$. realizando la división Euclidea de n entre d (Teorema A.2.3) existe $q,r \in \mathbb{Z}$ con $n = dq + r$ y $0 \leq r < d$. De acuerdo con la Notación I.1.4, se tiene que $a^n = a^{qd+r} = (a^d)^q a^r$. Como $a^d, a^n \in H$, deducimos que $a^r = a^n (a^d)^{-q} \in H$ porque H es un subgrupo. Como $0 \leq r < d$ y como $d = \text{mín}(A)$, concluimos que $r = 0$, luego $a^n = (a^d)^q \in < a^d >$.

En definitiva, $H =< a^d >$, luego H es cíclico. ■

Observación I.3.7 El recíproco no es cierto, es decir, existen grupos que no son cíclicos que contienen subgrupos cíclicos. Por ejemplo, en $(\mathbb{Q},+)$ se tiene que $\mathbb{Z} =< 1 >$ es un subgrupo cíclico.

I.3.2 Orden de un grupo y orden de un elemento

Definición I.3.8 Se llama **orden de un grupo** $(G,\cdot)$ al número de sus elementos. Si tiene infinitos elementos, escribimos $\#G=\infty$ y si tiene una cantidad finita de elementos, $\#G$ es igual al número de sus elementos.

Definición I.3.9 Sean $(G,\cdot)$ un grupo y $a\in G$. Se llama **orden de** a al entero positivo más pequeño m tal que $a^m=1_G$, si no existe dicho entero decimos que el **orden de** a **es infinito**. En ambos caso lo denotamos por $O(a)$, es decir,

- Si $\{m\in\mathbb{N}_{\geq 1}: a^m=1_G\}=\emptyset$, entonces $O(a)=\infty$.
- Si $\{m\in\mathbb{N}_{\geq 1}: a^m=1_G\}\neq\emptyset$, entonces $O(a)=\min\{m\in\mathbb{N}_{\geq 1}: a^m=1_G\}$.

Observación I.3.10 Comprobamos de forma directa $O(a)=1$ si y sólo si $a=1_G$, es decir, el elemento neutro es el único elemento de orden 1 de $(G,\cdot)$.

Proposición I.3.11 Sea $(G,\cdot)$ es un grupo finito. Entonces para todo $a\in G$ se tiene que el orden de a es finito, es decir, $O(a)<\infty$.

Demostración. Dado $a\in G$, como $<a>\subseteq G$, tenemos que $\#<a>\leq \#G<\infty$. Por consiguiente, existe $r\in\mathbb{N}_{\geq 1}$ tal que $\#<a>=r$. Por tanto, como $\#\{0,1,\ldots,r-1,r\}=r+1>r$, deben existir enteros $k,\ell\in\{0,1,\ldots,r-1,r\}$ con $k>\ell$ tales que $a^k=a^\ell$. Consecuentemente, se tiene que $a^{k-\ell}=1_G$ y, como $k-\ell\in\mathbb{N}_{\geq 1}$, se cumple que $\{m\in\mathbb{N}_{\geq 1}: a^m=1_G\}\neq\emptyset$, luego $O(a)<\infty$. ■

Ejemplos I.3.12 (1) $\#(\mathbb{C})=\#(\mathbb{R})=\#(\mathbb{Q})=\#(\mathbb{Z})=\infty$.

(2) Para cada $n\in\mathbb{N}_{\geq 1}$, $\#(\mathbb{Z}/n\mathbb{Z})=n$ y para cada $m\in\mathbb{N}_{\geq 1}$ se tiene que $\#(D_m)=2\cdot m$.

(3) ¡Ojo! Un mismo elemento puede tener órdenes distintos dependiendo del grupo y la operación. Por ejemplo, si tomamos $1_{\mathbb{R}}\in\mathbb{R}$ se tiene que $O(1)=\infty$ en $(\mathbb{R},+)$, porque $1+1+\cdots(\text{n veces})\cdots+1\neq 0$. Sin embargo $O(1)=1$ en $(\mathbb{R}\backslash\{0\},\cdot)$, porque $1^1=1$. Por ello, cuando exista posibilidad de ambigüedad porque tengamos más de una operación conviene especificar si hablamos de orden aditivo u orden multiplicativo.

De la misma forma comprobamos que $1_{\mathbb{Z}/n\mathbb{Z}}\in\mathbb{Z}/n\mathbb{Z}$ se tiene que $O(1)=n$ en $(\mathbb{Z}/n\mathbb{Z},+)$. Por ejemplo, también tenemos que $O(3)=3$ en $(\mathbb{Z}/9\mathbb{Z},+)$ porque $3\neq 0$, $3+3=6\neq 0$ pero $3+3+3=0$.

(4) En $(\mathbb{Z}/12\mathbb{Z},+)$ comprobamos realizando los cálculos pertinentes que $O(0)=1$, $O(1)=12$, $O(2)=6$, $O(3)=4$, $O(4)=3$, $O(5)=12$, $O(6)=2$, $O(7)=12$, $O(8)=3$, $O(9)=4$, $O(10)=6$ y que $O(11)=12$.

Propiedades I.3.13 — (sobre el orden de un elemento). Sea $(G,\cdot)$ un grupo y $a\in G$ un elemento con $O(a)=d\in\mathbb{N}_{\geq 1}$. Se cumple que:

(I) $<a>=\{a^0=1_G,a,a^2,\ldots,a^{d-1}\}$.

(II) $\#<a>=O(a)=d$.

(III) Para todo $t\in\mathbb{Z}$ se tiene que $a^t=1$ si y sólo si $d\mid t$ (escrito de otro modo $O(a)\mid t$).

(IV) Para todos $m,n\in\mathbb{Z}$ se tiene que $a^m=a^n$ si y sólo si $m\equiv n\,(\text{mód}\,d)$.

(V) Para todo $k\in\mathbb{N}_{\geq 1}$ se tiene que $O(a^k)=\dfrac{O(a)}{\text{m.c.d.}\,(O(a),k)}=\dfrac{d}{\text{m.c.d.}\,(d,k)}$.

Demostración. (I) Como $< a >= \{a^n : n \in \mathbb{Z}\}$ (ver Observación I.2.14), se tiene que

$$\{a^0 = 1_G, a, a^2, \ldots, a^{d-1}\} \subseteq < a > .$$

Veamos que $< a > \subseteq \{a^0 = 1_G, a, a^2, \ldots, a^{d-1}\}$. Dado $x \in < a >$, existe $n \in \mathbb{Z}$ tal que $x = a^n$. Realizando la división euclídea (Teorema A.2.3) de n entre d, existe $q, r \in \mathbb{Z}$ tales que $n = qd + r$ con $0 \leq r < d$. Por tanto, por la Notación I.1.4 y, como $O(a) = d$, $a^d = 1_G$ y se tiene que:

$$a^n = a^{qd+r} = (a^d)^q a^r = (1_G)^q a^r = 1_G\, a = a^r.$$

Dado que $0 \leq r < d$, hemos probado que $a^n = a^r \in \{a^0 = 1_G, a, a^2, \ldots, a^{d-1}\}$ y concluimos que $< a >= \{a^0 = 1_G, a, a^2, \ldots, a^{d-1}\}$.

(II) En primer lugar, vemos que los elementos $a^0 = 1_G, a, a^2, \ldots, a^{d-1}$ son distintos dos a dos. Razonamos por reducción al absurdo y suponemos que $a^t = a^s$ con $t, s \in \{0, 1, \ldots, d-1\}$ y $s < t$. Tendríamos que $a^{t-s} = 1_G$ con $0 < t - s < d$ en contradiciendo que $d = \text{mín}\{k \in \mathbb{N}_{\geq 1} : a^k = 1_G\}$. Luego $\#\{a^0 = 1_G, a, a^2, \ldots, a^{d-1}\} = d$ y, por (I), concluimos que

$$\# < a >= \#\{a^0 = 1_G, a, a^2, \ldots, a^{d-1}\} = O(a) = d.$$

(III) Dado $t \in \mathbb{Z}$, realizando la división euclídea (Teorema A.2.3) de t entre d existen $q, r \in \mathbb{Z}$ tales que $t = qd + r$ con $0 \leq r < d$. Como $d = O(a)$, se tiene que $a^t = a^r$ y, en consecuencia, vemos que

$$a^t = 1_G \quad \Leftrightarrow \quad a^r = 1_G \quad \overbrace{\Leftrightarrow}^{0 \leq r < d,\, d = O(a)} \quad r = 0 \quad \overbrace{\Leftrightarrow}^{t = qd + r} \quad d \mid t.$$

(IV) Para todos $m, n \in \mathbb{Z}$ se tiene que

$$a^m = a^n \quad \Leftrightarrow \quad a^{m-n} = 1_G \quad \overbrace{\Leftrightarrow}^{\text{(III)}} \quad d \mid (m-n) \quad \Leftrightarrow \quad m \equiv n \,(\text{mód}\, d).$$

(V) Dado $k \in \mathbb{N}_{\geq 1}$, como $a^k \in < a >$ y $\# < a >= d < \infty$ por (II), $O(a^k) = m < \infty$ (Proposición I.3.11). Denotamos por $f := \text{m.c.d.}\,(d, k) \in \mathbb{N}_{\geq 1}$ y de acuerdo con el Corolario A.2.13, $d = fd_1$ y $k = fk_1$ con $\text{m.c.d.}\,(d_1, k_1) = 1$. Veamos que $m = O(a^k) = d_1$. Observamos que

$$(a^k)^{d_1} = a^{kd_1} = a^{fk_1 d_1} = a^{dk_1} = (a^d)^{k_1} = 1_G.$$

En consecuencia, por (III), se tiene que $m \mid d_1$.
Veamos ahora que $d_1 \mid m$. Como $(a^k)^m = 1_G$, se tiene que $a^{km} = 1_G$ y, por (III), $O(a) \mid km$. En otras palabras, $d \mid km$ o, equivalentemente, $fd_1 \mid fk_1 m$. Por las propiedades de divisibilidad en $\mathbb{Z}$, $d_1 \mid k_1 m$ y como $\text{m.c.d.}\,(d_1, k_1) = 1$, concluimos que $d_1 \mid m$ (Corolario A.2.13). En resumen, $O(a^k) \mid d_1$ y $d_1 \mid O(a^k)$ y ambos son naturales, se cumple que $O(a^k) = d_1$ (ver Observación A.2.2), es decir,

$$O(a^k) = d_1 = \frac{d}{f} = \frac{d}{\text{m.c.d.}\,(d, k)} = \frac{O(a)}{\text{m.c.d.}\,(O(a), k)}.$$

■

Ejemplos I.3.14 (1) Calcular el orden de 6 en $(\mathbb{Z}/20\mathbb{Z}, +)$. Podemos proceder empleando el apartado (II) de la proposición anterior. Observamos que

$$< 6 >= \{0 = 0 \cdot 6,\ 6 = 1 \cdot 6,\ 12 = 2 \cdot 6 = 6 + 6,\ 18,\ 4,\ 10,\ 16,\ 2,\ 8,\ 14\},$$

luego $O(6) = \# < 6 >= 10$.

(2) Calcular el orden de 6 en $(\mathbb{Z}/40\mathbb{Z},+)$. Podemos proceder empleando el apartado (V) de la proposición anterior. Como $6 = 1+1+1+1+1+1 = 6\cdot 1$, y como $O(1) = 40$ porque $\mathbb{Z}/40\mathbb{Z} =< 1 >$, se tiene que

$$O(6) = O(6\cdot 1) = \frac{O(1)}{\text{m.c.d.}\,(O(1),6)} = \frac{40}{2} = 20.$$

En ambos casos, nótese que, como la operación es la suma, se está empleando la versión aditiva de la proposición anterior (ver Notación I.1.4).

I.3.3 Grupos cíclicos finitos

Proposición I.3.15 Sea $(G,\cdot)$ un grupo finito, es decir, $\#G < \infty$. Se cumple que:

G es cíclico si y sólo si existe $a \in G$ tal que $O(a) = \#G$.

Demostración. En primer lugar, supongamos que G es cíclico, luego existe $a \in G$ tal que $G =< a >$. Por la Proposición I.3.11, como $\#G < \infty$, tenemos que $O(a) < \infty$. Finalmente por la Propiedad I.3.13.(II), concluimos $\#G = \# < a >= O(a)$.
Recíprocamente, supongamos que existe $a \in G$ tal que $O(a) = \#G$. Por la Propiedad I.3.13.(II), $\# < a >= O(a)$. Por consiguiente, $< a > \subseteq G$ y $\# < a >= \#G$ y deducimos que $G =< a >$. En otras palabras, hemos probado que existe $a \in G$ tal que $G =< a >$, es decir, G es cíclico. ■

Propiedades I.3.16 — (Grupos cíclicos finitos). Sea $(G,\cdot)$ un grupo cíclico finito, es decir, $\#G = n \in \mathbb{N}_{\geq 1}$ y existe $a \in G$ tal que $G =< a >$. Se cumple que:

(I) dado $k \in \mathbb{Z}$, se tiene que $G =< a^k >$ (a^k es generador de G) si y solo si $\text{m.c.d.}\,(k,n) = 1$.

(II) el número de elementos de orden n en G es $\varphi(n)$, donde φ es la Función de Euler dada por $\varphi(n) = \#\{x \in \mathbb{N} : x < n \ y \ \text{m.c.d.}\,(x,n) = 1\}$ (ver Ejercicio A.2.28).

(III) el orden de cualquier subgrupo de G divide a $\#G$.

(IV) para cualquier $d \in \mathbb{N}$ divisor de n, G posee sólo un subgrupo de orden d: $G_d :=< a^{n/d} >$.

(V) para cualquier $d \in \mathbb{N}$ divisor de n, se cumple la igualdad $G_d = \{b \in G : O(b) \mid d\}$, es decir, G_d coincide con el conjunto de elementos de G cuyo orden divide a d.

Demostración. Por la Propiedad I.3.13.(II), sabemos que $O(a) = \#G = n$.

(I) En primer lugar, observamos que, se tiene que $O(a^k) = O(a)/\text{m.c.d.}\,(O(a),k) < \infty$, por la Propiedad I.3.13.(V). Como G es finito se cumple que $G =< a^k >$ si y solo si $\#G = \# < a^k >$, y, por la Propiedad I.3.13.(II), si y solo si $\#G = O(a^k)$. Empleando la fórmula para el orden y como $\#(G) = O(a) = n$, se tiene que $G = O(a^k)$ si y solo si

$$\frac{O(a)}{\text{m.c.d.}\,(O(a),k)} = \#(G) \quad \Leftrightarrow \quad \frac{n}{\text{m.c.d.}\,(n,k)} = n \quad \Leftrightarrow \quad \text{m.c.d.}\,(n,k) = 1.$$

(II) Por la Propiedad I.3.13.(I), tenemos que $G =< a >= \{1 = a^0, a, \ldots, a^{n-1}\}$. Por tanto, usando el apartado (I), deducimos que el número de elementos de orden n, es el número de elementos $k \in \{0,\ldots,n-1\}$ tales que $\text{m.c.d.}\,(k,n) = 1$, es decir, $\varphi(n)$.

(III) Si S es un subgrupo de G, por la Proposición I.3.6, S es cíclico. Como los elementos de G son potencias de a, existe $\ell \in \mathbb{Z}$ tal que $S =< a^\ell >$ y por la Propiedad I.3.13.(II) tenemos que $\#S = \# < a^\ell >= O(a^\ell)$. Por la Propiedad I.3.13.(V), deducimos que

$$\#S = O(a^\ell) = \frac{O(a)}{\text{m.c.d.}\,(\ell, O(a))} = \frac{\#G}{\text{m.c.d.}\,(\ell, \#G)},$$

y deducimos que $(\#S)\,(\text{m.c.d.}\,(\ell, \#G)) = \#G$, es decir, $\#S \mid \#G$.

(IV) Dado $d \in \mathbb{N}_{\geq 1}$ tal que $d \mid n$, se tiene que existe $q \in \mathbb{N}_{\geq 1}$ tal que $n = dq$. Por la Propiedad I.3.13.(V), observamos que

$$O(a^q) = \frac{O(a)}{\text{m.c.d.}\,(O(a), q)} = \frac{n}{\text{m.c.d.}\,(dq, q)} = \frac{n}{q} = d.$$

Por consiguiente, por la Propiedad I.3.13.(II), $S =< a^q >=< a^{n/d} >$ es un subgrupo de orden d. Veamos que S es el único. Dado T un subgrupo de G de orden d, por la Proposición I.3.6, T es cíclico y, como los elementos de G son potencias de a, existe $m \in \mathbb{Z}$ tal que $T =< a^m >$. Veamos que $a^m \in G_d$. Como $\#T = d$, por la Propiedad I.3.13.(II), $O(a^m) = d$, luego $a^{md} = 1_G$ y, de la Propiedad I.3.13.(III), deducimos que $O(a) \mid md$. Por tanto $qd \mid md$, luego $q \mid m$, es decir, existe $t \in \mathbb{Z}$ tal que $qt = m$. Empleando esta igualdad, vemos que $a^m = a^{qt} = (a^q)^t$, luego $a^m \in < a^q >$ y, por este motivo, $T =< a^m > \subseteq < a^q >= S$. Finalmente, como $\#T = \#S = d$, concluimos que $T = S$, es decir, el subgrupo es único.

(V) Dado $b \in G_d =< a^{n/d} >$, $b = (a^{n/d})^m$ para algún $m \in \mathbb{Z}$ y observamos que $b^d = ((a^{n/d})^m)^d = (a^n)^m = (1_G)^m = 1_G$. Por la Propiedad I.3.13.(III), se tiene que $O(b) \mid d$ y, consecuentemente, que $G_d \subseteq \{b \in G : O(b) \mid d\}$.
Recíprocamente, dado $b \in G$ un elemento con $O(b) = \ell$ y $\ell \mid d$, es decir, $d = \ell k$ para algún $k \in \mathbb{N}_{\geq 1}$, por la Propiedad I.3.13.(II), $< b >$, es un subgrupo de G de orden $O(b) = \ell$. Por (IV), $< b >= G_\ell =< a^{n/\ell} >$ y, como $a^{n/\ell} = (a^{n/d})^k$, deducimos que $< b >= G_\ell \subseteq G_d$. En consecuencia, concluimos que $b \in G_d$ y que $G_d = \{b \in G : O(b) \mid d\}$. ■

Ejemplo I.3.17 Podemos emplear las propiedades anteriores para determinar todos los subgrupos de $(U(\mathbb{Z}/9\mathbb{Z}), \cdot)$ (ver Ejercicio I.1.7). Comprobamos que $U(\mathbb{Z}/9\mathbb{Z}) = \{1,2,4,5,7,8\}$ y que $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 7$ y que $2^6 = 5$. En consecuencia, $U(\mathbb{Z}/9\mathbb{Z}) =< 2 >$, es decir, $(U(\mathbb{Z}/9\mathbb{Z}), \cdot)$ es un grupo cíclico de orden 6. De acuerdo, con las Propiedades I.3.16.(III) y (IV), $U(\mathbb{Z}/9\mathbb{Z})$ tiene:

- un único subgrupo de orden 1, $< 2^{6/1} >=< 1 >= \{1\}$,
- un único subgrupo de orden 2, $< 2^{6/2} >=< 8 >= \{1,8\}$,
- un único subgrupo de orden 3, $< 2^{6/3} >=< 4 >= \{1,4,7\}$,
- un único subgrupo de orden 6, $< 2^{6/6} >=< 2 >= U(\mathbb{Z}/9\mathbb{Z}) = \{1,2,4,5,7,8\}$,

Si queremos encontrar los generadores de $U(\mathbb{Z}/9\mathbb{Z})$, empleando la Propiedad I.3.16.(II), vemos que el número de elementos de orden 6 de G, es $\varphi(6) = 2$. En concreto, comprobamos que $U(\mathbb{Z}/9\mathbb{Z}) =< 2 >$ y $U(\mathbb{Z}/9\mathbb{Z}) =< 5 >$.

Teorema I.3.18 Sea $(G, \bullet)$ un grupo con más de un elemento. Se cumple que
G es cíclico de orden primo si y solo si sus únicos subgrupos son $\{1_G\}$ y G.

Demostración. En primer lugar, supongamos que G es cíclico de orden primo. Por la Proposición A.2.20, los únicos divisores positivos de $\#G$ son 1 y $\#G$. Por las Propiedades I.3.16.(III) y (IV), G tiene únicamente dos subgrupos uno de orden 1 y otro de orden $\#G$, es decir, sus únicos subgrupos son $\{1_G\}$ y G.

Recíprocamente, supongamos que los únicos subgrupos de G son $\{1_G\}$ y G. Como G tiene más de un elemento, existe $a \in G$ con $a \neq 1_G$. Tenemos que $< a >$ es un subgrupo de G, luego por hipótesis, o bien $< a >= \{1_G\}$ o bien $< a >= G$. Como $a \neq 1_G$, deducimos que $G =< a >$, es decir, G es cíclico. Veamos ahora que $O(a) < \infty$. Distinguimos dos casos:

(a) Si $a^2 = 1_G$, tenemos que $O(a) = 2$ y hemos terminado.

(b) Si $a^2 \neq 1_G$, como $< a^2 >$ es un subgrupo de G, por hipótesis, necesariamente tenemos que $< a^2 >= G$. Por tanto, $a \in < a^2 >$ y, en consecuencia, existe $q \in \mathbb{Z}$ tal que $a = a^{2q}$, luego $a^{2q-1} = 1_G$. Como o bien $2q-1 \in \mathbb{N}_{\geq 1}$ o bien $-(2q-1) \in \mathbb{N}_{\geq 1}$, concluimos que existe $\ell \in \mathbb{Z}$ tal que $a^\ell = 1_G$, luego $O(a) < \infty$.

En consecuencia, por la Propiedad I.3.13.(II) tenemos que $\#G = \# < a >= O(a) < \infty$, es decir, G es cíclico de orden finito. Por la Propiedad I.3.16.(IV) para cada divisor positivo d de $\#G$, existe un único subgrupo de orden d y, como los únicos subgrupos de G son $\{1_G\}$ y G, concluimos que los únicos divisores de $\#G$ son 1 y $\#G$. Finalmente, por la Proposición A.2.20, $\#G$ es primo. ■

Ejercicio I.3.19 Probar que $(\mathbb{Z},+) \times (\mathbb{Z},+)$ (ver Ejercicio I.1.9) es abeliano pero no es cíclico.

Ejercicio I.3.20 Dado $n \in \mathbb{N}_{\geq 1}$ y $a \in \mathbb{Z}/n\mathbb{Z}$, si $O(a)$ es el orden de a en $(\mathbb{Z}/n\mathbb{Z},+)$. Probar que $O(a) \cdot \text{m.c.d.}(n,a) = n$

Ejercicio I.3.21 Si a,b son elementos de un grupo $(G,\cdot)$, probar que:

$$(1)\, O(a) = O(a^{-1}), \quad (2)\, O(ab) = O(ba) \quad (3)\, O(a) = O(bab^{-1}).$$

Ejercicio I.3.22 Sea $(G,\cdot)$ un grupo y $a,b \in G$ tales que $O(a) = m$, $O(b) = n$ y $ab = ba$. Probar que:

(I) $O(ab)$ es divisor de $\text{m.c.m.}(n,m)$.

(II) Si $\text{m.c.d.}(m,n) = 1$, entonces $O(ab) = mn$.

(III) Deducir de (II) que si G es abeliano y finito, entonces existe un elemento $c \in G$ tal que $O(c) = \text{m.c.m.}(\{O(a) : a \in G\})$.

Ejercicio I.3.23 Determinar dos elementos a,b de $(\mathbb{Z}/12\mathbb{Z},+)$ de forma que $O(a+b)$ sea divisor propio de $m.c.m\{O(a),O(b)\}$, es decir, en el Ejercicio I.3.22.(I) la condición de divisibilidad puede ser estricta.

Probar que la condición $ab = ba$ en el Ejercicio I.3.22.(I) es necesaria. (Pista: buscar en D_3 elementos a,b de forma que E. I.3.22.(I) no se cumple).

Ejercicio I.3.24 Consideramos el grupo de isometrías afines en un espacio afín euclideo real de dimensión 3, con composición. Consideramos dos elementos de este grupo representados por:

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Calcular $O(A)$, $O(B)$ y $O(AB)$. (Nota: Observamos que A y B representan simetrías ortogonales respecto a planos paralelos en el espacio afín euclideo de dimensión 3 y su composición es una translación. Dos espejos situados uno frente al otro reproducen la situación descrita en este ejemplo)

Ejercicio I.3.25 Sean $(G,\bullet_{|G})$ y $(H,\bullet_{|H})$ dos grupos y $g\in G$, $h\in H$ dos elementos tales que $O(g)=n$ y $O(h)=m$ con $n,m\in\mathbb{N}_{\geq 1}$. Probar que el orden de (g,h) en $G\times H$ (ver Ejercicio I.1.9) es $O((g,h))=\text{m.c.m.}\,(O(g),O(h))=\text{m.c.m.}\,(n,m)$.

Empleando lo anterior, calcular el orden de $(2,9)$ en $(\mathbb{Z}/10\mathbb{Z},+)\times(\mathbb{Z}/11\mathbb{Z},+)$.

Ejercicio I.3.26 Sea $(G,\bullet)$ un grupo cíclico infinito, es decir, $\#G=\infty$ tal que existe $a\in G$ con $G=<a>$. Probar que a y a^{-1} son los únicos generadores de G.

Ejercicio I.3.27 Probar que todo grupo cíclico infinito posee infinitos subgrupos.

Ejercicio I.3.28 Probar que todo grupo que sólo posee un número finito de subgrupos, debe ser finito.

Ejercicio I.3.29 Sea $G=\{x\in\mathbb{Q}\,:\,0\leq x<1\}$, se define

$$x*y=\begin{cases} x+y & \text{si} \quad x+y<1,\\ x+y-1 & \text{si} \quad x+y\geq 1.\end{cases}$$

Probar que $(G,*)$ es un grupo abeliano infinito en el cual todos los elementos tienen orden finito.

I.4 Grupos de permutaciones

Definición I.4.1 Sea X un conjunto no vacío. Llamamos **permutación** a toda aplicación biyectiva $\sigma:X\to X$.

Definición I.4.2 Sea X un conjunto no vacío. Se comprueba de forma directa que el conjunto de permutaciones de X, aplicaciones biyectivas de X en X, con la composición de aplicaciones como ley es un grupo. Este grupo se denomina **grupo de permutaciones de** X y si denotamos al conjunto de permutaciones por $S(X)$, es decir,

$$S(X):=\{\sigma:X\to X\,:\,\sigma \text{ es biyectiva}\},$$

tenemos que el grupo de permutaciones es $(S(X),\circ)$.

Definición I.4.3 El grupo de permutaciones de $I_n=\{1,2,\ldots,n\}$, se denomina **grupo simétrico** y el conjunto de permutaciones se denota por

$$S_n:=S(\{1,2,\ldots,n\})=\{\sigma:\{1,2,\ldots,n\}\to\{1,2,\ldots,n\}\,:\,\sigma\text{es biyectiva}\}.$$

Si X un conjunto finito con $n\in\mathbb{N}_{\geq 1}$ elementos, se comprueba que $S(X)$ es isomorfo a S_n.

Ejemplo I.4.4 $(S_3,\circ)$ es un grupo con 6 elementos. Si $I_3=\{1,2,3\}$, lo elementos de S_3 son

$\sigma_A:I_3\to I_3$	$\sigma_B:I_3\to I_3$	$\sigma_C:I_3\to I_3$	$\sigma_D:I_3\to I_3$	$\sigma_E:I_3\to I_3$	$\sigma_F:I_3\to I_3$
$1\to 1$	$1\to 2$	$1\to 3$	$1\to 2$	$1\to 3$	$1\to 1$
$2\to 2$	$2\to 3$	$2\to 1$	$2\to 1$	$2\to 2$	$2\to 3$
$3\to 3$	$3\to 1$	$3\to 2$	$3\to 3$	$3\to 1$	$3\to 2$

Observación I.4.5 En general, tenemos que $(S_n,\circ)$ es un grupo finito de orden $n!$.

Notación I.4.6 Un elemento $\sigma \in S_n$ es una aplicación $\sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ biyectiva, y por tanto, queda completamente determinada por la imagen de todos los elementos de $\{1,2,\ldots,n\}$. Por ejemplo en S_5, consideramos:

$$\sigma_1(1)=2, \quad \sigma_1(2)=4, \quad \sigma_1(3)=3, \quad \sigma_1(4)=5, \quad \sigma_1(5)=1.$$
$$\sigma_2(1)=5, \quad \sigma_2(2)=4, \quad \sigma_2(3)=1, \quad \sigma_2(4)=2, \quad \sigma_2(5)=3.$$

En este contexto, σ_1 y σ_2 se expresan de modo abreviado, en dos lineas, como:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix},$$

donde debajo de cada j se sitúa $\sigma(j)$. De este modo resulta sencillo determinar el resultado de componer dos o más permutaciones: basta con recorrer de derecha a izquierda la cadena de expresiones moviéndonos de arriba abajo en cada una de ellas. Por ejemplo:

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & \downarrow & & & \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}.$$

Existe un tipo elemental de permutación mediante el cual podemos representar permutaciones más complejas.

Definición I.4.7 Sean $i_1, i_2, \ldots, i_\ell$ elementos de $I_n = \{1,2,\ldots,n\}$ distintos dos a dos. Se representa por $(i_1, i_2, i_3, \ldots, i_\ell)$ a la permutación que aplica

$$i_1 \to i_2, \qquad i_2 \to i_3, \qquad \ldots\ldots, \qquad i_{\ell-1} \to i_\ell, \qquad i_\ell \to i_1.$$

y que deja fijos los elementos de $I_n \backslash \{i_1, i_2, \ldots, i_\ell\}$. Este tipo de permutaciones se llaman **ciclos de longitud** ℓ.
Los ciclos de longitud 2 se denominan **transposiciones**.

Ejemplo I.4.8 En S_5 el ciclo que se denota por $(4,3,1)$ representa la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}.$$

Observación I.4.9 A la hora de expresar un ciclo da igual elemento que tomemos como elemento inicial siempre que se mantenga el mismo orden de los elementos, es decir, $(i_1, i_2, i_3, \ldots, i_\ell) = (i_2, i_3, \ldots, i_\ell, i_1) = (i_3, \ldots, i_\ell, i_1, i_2) = \cdots = (i_\ell, i_1, i_2, \ldots, i_{\ell-1})$.
El inverso de un ciclo $(i_1, i_2, i_3, \ldots, i_\ell)$ en S_n es $(i_\ell, i_{\ell-1}, \ldots, i_2, i_1)$.

Definición I.4.10 Sean $\sigma_1, \sigma_2, \ldots, \sigma_s$ permutaciones de S_n. Se dice que $\sigma_1, \sigma_2, \ldots, \sigma_s$ son **disjuntas** si para cada $j \in \{1,2,\ldots,s\}$ y cada $k \in I_n = \{1,2,\ldots,n\}$ se tiene que

$$\text{Si } \sigma_j(k) \neq k, \qquad \text{entonces} \qquad \forall i \in \{1,2,\ldots,s\}, \quad i \neq j, \quad \sigma_i(k) = k.$$

Dicho de otra forma, si σ_j no deja fijo k, entonces el resto de permutaciones dejan fijo a k.

Para probar el resultado principal, descomposición en cíclos disjuntos, necesitamos el siguiente resultado auxiliar.

Proposición I.4.11 Sean $\sigma, \tau \in S_n$ dos permutaciones disjuntas. Entonces σ y τ conmutan, es decir,

$$\sigma \circ \tau = \tau \circ \sigma.$$

Demostración. Dado $k \in \{1,2,\dots,n\}$, distinguimos 3 casos:

(a) Si k es fijo por σ y τ: $\sigma(\tau(k)) = \sigma(k) = k = \tau(k) = \tau(\sigma(k))$.

(b) Si k es movido por σ ($\sigma(k) \neq k$), como σ y τ son disjuntas, k es fijo para τ, es decir, $\tau(k) = k$. Definimos $\ell := \sigma(k) \neq k$ y observamos que

$$\sigma(\tau(k)) = \sigma(k) = \ell,$$

$$\tau(\sigma(k)) = \tau(\ell) = \begin{cases} \text{o bien } \tau(\ell) = \ell. \\ \text{o bien } \tau(\ell) \neq \ell \end{cases} \overset{\sigma,\,\tau \text{ disjuntos}}{\Rightarrow} \sigma(\ell) = \ell \overset{\sigma \text{ biyectiva}}{\Rightarrow} \underset{\text{(absurdo)}}{k = \ell}.$$

Luego $\sigma(\tau(k)) = \ell = \tau(\sigma(k))$.

(c) Si k es movido por τ (Análogo a (b)).

Por consiguiente, hemos probado que para todo $k \in \{1,2,\dots,n\}$, se tiene que $\sigma(\tau(k)) = \tau(\sigma(k))$, luego $\sigma \circ \tau = \tau \circ \sigma$. ■

Teorema I.4.12 (Descomposición de permutaciones). Sea $\sigma \in S_n$ con $\sigma \neq \mathrm{Id}$. Entonces o σ es un ciclo o es una composición de ciclos disjuntos.

Además esta descomposición es única salvo reordenación de los ciclos.

Demostración. EXISTENCIA

Como $\sigma \neq \mathrm{Id}$, existe $a \in \{1,2,\dots,n\}$ tal que $\sigma(a) \neq a$. Establecemos la siguiente notación:

$$a_0 := a, \quad a_1 := \sigma(a_0), \quad a_2 := \sigma(a_1) = \sigma^2(a_0), \quad \dots \quad a_m := \sigma(a_{m-1}) = \sigma^m(a_0), \quad \dots$$

Como el conjunto $\{1,2,\dots,n\}$ es finito, existen $m, \ell \in \mathbb{Z}$ con $0 \leq \ell < m$ tal que $a_m = a_\ell$. En otras palabras, se tiene que $\sigma^m(a_0) = \sigma^\ell(a_0)$ y aplicando σ^{-1} a ambos ℓ veces vemos que $\sigma^{m-\ell}(a_0) = a_0$.

Por tanto $\{s \in \mathbb{N}_{\geq 1} \,:\, \sigma^s(a_0) = a_0\} \neq \emptyset$ y, por el Principio de Buena Ordenación, podemos considerar $r = \min\{s \in \mathbb{N}_{\geq 1} \,:\, \sigma^s(a_0) = a_0\}$. Como r es el mínimo, tenemos que $a_m \neq a_\ell$ si $0 \leq \ell < m \leq r-1$: en caso contrario, razonando como antes, tendríamos que $\sigma^{m-\ell}(a_0) = a_0$ lo que es imposible porque $m - \ell \leq m < r$. En consecuencia, podemos considerar el siguiente ciclo de longitud r:

$$a = a_0 \to a_1, \qquad a_1 \to a_2, \qquad \dots\dots, \qquad a_{r-2} \to a_{r-1}, \qquad a_{r-1} \to a_r = a,$$

es decir, $(a_0, a_1, \dots, a_{r-1})$.

Tenemos dos opciones:

Si $\sigma(x) = x$ para todo $x \in \{1,2,\dots,n\} \backslash \{a_0, a_1, \dots, a_{r-1}\}$, entonces $\sigma = (a_0, a_1, \dots, a_{r-1})$ y hemos terminado.

Si existe $b \in \{1,2,\dots,n\} \backslash \{a_0, a_1, \dots, a_{r-1}\}$ tal que $\sigma(b) \neq b$. Repetimos el procedimiento y tomando $b_0 = b$ construimos el ciclo $(b_0, b_1, \dots, b_{s-1})$. Veamos que este ciclo es disjunto con el anterior. Razonamos por reducción al absurdo si $a_m = b_\ell$ tendríamos que $\sigma^m(a_0) = \sigma^\ell(b_0)$, entonces $\sigma^{m-\ell}(a_0) = b_0$ luego se tendría que $b_0 \in \{a_0, a_1, \dots, a_{r-1}\}$, lo que es imposible.

Como $\{1,2,\dots,n\}$ es finito iterando el procedimiento y en un número finito de pasos descomponemos σ como

$$\sigma = (a_0, a_1, \dots, a_{r-1})(b_0, b_1, \dots, b_{s-1}) \cdots (y_0, y_1, \dots, y_{t-1}),$$

donde los ciclos son disjuntos.

UNICIDAD

Dada $\sigma \in S_n$ una permutación distinta de la identidad y sean $\sigma_1, \sigma_2, \ldots, \sigma_r$ y $\tau_1, \tau_2, \ldots, \tau_s$ dos conjuntos de **ciclos disjuntos** tales que

$$\sigma_1\sigma_2\cdots\sigma_r = \sigma = \tau_1\tau_2\cdots\tau_s.$$

Sin pérdida de generalidad suponemos que $s \geq r$.

Como $\sigma \neq \mathrm{Id}$ existe $k \in \{1,2,\ldots,n\}$, tal que $\sigma(k) \neq k$. Por tanto, existe un $i_0 \in \{1,2,\ldots,r\}$ tal que $\sigma_{i_0}(k) \neq k$ y un $j_0 \in \{1,2,\ldots,s\}$ tal que $\tau_{j_0}(k) \neq k$.

Como los **ciclos disjuntos conmutan**, Proposición I.4.11, podemos suponer que $\sigma_1(k) \neq k$ y que $\tau_1(k) \neq k$, sin pérdida de generalidad. Por otro lado, por la definición de ciclos disjuntos como σ_1 y τ_1 no dejan fijo a k, entonces σ_i y τ_j dejan fijo a k para todo $i \in \{2,3,\ldots,r\}$ y todo $j \in \{2,3,\ldots,s\}$ y, por este motivo, se tiene que $\sigma_1(k) = \sigma(k) = \tau_1(k)$.

Empleando de nuevo que los **ciclos disjuntos conmutan**, Proposición I.4.11, observamos que

$$\sigma\tau_1 = \tau_1\tau_2\cdots\tau_s\tau_1 = \tau_1^2\tau_2\cdots\tau_s = \tau_1\sigma.$$

Como $\sigma(k) = \tau_1(k)$, resulta que

$$\sigma^2(k) = \sigma(\sigma(k)) = \sigma(\tau_1(k)) = \tau_1(\sigma(k)) = \tau_1(\tau_1(k)) = \tau_1^2(k).$$

Análogamente, como $\sigma(k) = \sigma_1(k)$, vemos que $\sigma^2(k) = \sigma_1^2(k)$. Mediante un proceso inductivo, probamos que

$$(\star) \qquad \text{para todo} \quad n \in \mathbb{N}_{\geq 1} \quad \text{se cumple que} \quad \sigma_1^n(k) = \sigma^n(k) = \tau_1^n(k).$$

Ahora como σ_1 es un **ciclo**, $\sigma_1 = (k_1, k_2, \ldots, k_m)$, con $k_i \in \{1,2,\ldots,n\}$, es decir, σ_1 envía k_i en k_{i+1} para todo $i \in \{1,2,\ldots,m-1\}$, envía k_m en k_1 y deja fijo a todos los elementos ℓ de $\{1,2,\ldots,n\}$ que no están en el subconjunto $\{k_1, k_2, \ldots, k_m\}$.

Como σ_1 no deja fijo al elemento k, podemos afirmar que $k \in \{k_1, k_2, \ldots, k_m\}$. Por ello, podemos escribir $k = k_i$ para algún $i \in \{1,2,\ldots,m\}$, como podemos reescribir el ciclo comenzando en el elemento que queramos

$$\sigma_1 = (k_1, k_2, \ldots, k_t) = (k_i, k_{i+1}, \ldots, k_{i-1}) = (k, \sigma_1^1(k), \ldots, \sigma_1^{m-1}(k)).$$

Del mismo modo, como τ_1 es ciclo tenemos que $\tau_1 = (k, \tau_1^1(k), \ldots, \tau_1^{t-1}(k))$. Aplicando la propiedad $(\star)$, concluimos que $m = t$ y que

$$\sigma_1 = (k, \sigma_1^1(k), \ldots, \sigma_1^{m-1}(k)) = (k, \sigma^1(k), \ldots, \sigma^{m-1}(k)) = (k, \tau_1^1(k), \ldots, \tau_1^{m-1}(k)) = \tau_1.$$

Por consiguiente, como $\tau_1 = \sigma_1$, deducimos que $(\tau_1)^{-1} = (\sigma_1)^{-1}$. Como por hipótesis sabemos que $\sigma_1\sigma_2\cdots\sigma_r = \tau_1\tau_2\cdots\tau_s$, multiplicando a ambos lados por $(\sigma_1)^{-1}$, vemos que

$$\sigma_2\cdots\sigma_r = \tau_2\cdots\tau_s.$$

Como r es finito, repitiendo el proceso r veces, vemos que para cada $i \in \{1,2,\ldots,r\}$ existe un $j \in \{1,2,\ldots,s\}$ tal que $\sigma_i = \tau_j$. Finalmente, razonando por reducción al absurdo si $s > r$ (desigualdad estricta), tras r pasos tendríamos que $\mathrm{Id} = \tau_{r+1}\cdots\tau_{s-1}\tau_s$. Consecuentemente, se deduciría que $\tau_s^{-1} = \tau_{r+1}\cdots\tau_{s-1}$, lo que es imposible porque los ciclos son disjuntos. Por esta razón, concluimos que $s = r$. ■

Ejemplo I.4.13 En S_{15} consideramos la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 7 & 11 & 15 & 9 & 14 & 2 & 4 & 10 & 13 & 5 & 6 & 12 & 1 & 8 & 3 \end{pmatrix}.$$

Observamos que σ decompone en ciclos como

$$\sigma = (1 \;\; 7 \;\; 4 \;\; 9 \;\; 13)\,(2 \;\; 11 \;\; 6)\,(3 \;\; 15)\,(5 \;\; 14 \;\; 8 \;\; 10).$$

Por esta proposición podemos relacionar el orden de una permutación como elemento de $(S_n, \circ)$ con el orden de los ciclos en los que descompone.

Proposición I.4.14 Sean $\sigma \in S_n$ un ciclo de longitud ℓ. Entonces $O(\sigma) = \ell$ en $(S_n, \circ)$.

Demostración. Tenemos que $\sigma = (i_1, i_2, \ldots, i_\ell)$. Comprobamos que para todo $k \in \{1, 2, \ldots, n\}$ se cumple que $\sigma^\ell(k) = k$. Por tanto, $\sigma^\ell = \mathrm{Id}$ y deducimos que $O(\sigma) \mid \ell$ por la Propiedad I.3.13.(III). Por otro lado, si $\sigma^m = \mathrm{Id}$, tenemos que $\sigma^m(j) = j$ para todo $j \in \{i_1, i_2, \ldots, i_\ell\}$, entonces $i_{(k+m \mod \ell)} = i_k$ para todo $k \in \{1, \ldots, \ell\}$. Como los elementos del ciclo son distintos dos a dos eso quiere decir que $k + m \equiv k \mod \ell$, luego $\ell \mid m$, es decir, $\ell \mid O(\sigma)$. En consecuencia, se tiene que $\ell = O(\sigma)$ (ver ObservaciónA.2.2). ■

Corolario I.4.15 Sea $\sigma \in S_n$ una permutación y $\sigma_1, \sigma_2, \ldots, \sigma_s \in S_n$ ciclos disjuntos de longitudes respectivas $\ell_1, \ell_2, \ldots, \ell_s \in \mathbb{N}_{\geq 1}$ tales que $\sigma = \sigma_1 \sigma_2 \cdots \sigma_s$. Entonces se cumple que

$$O(\sigma) = \text{m.c.m.}\,(\ell_1, \ell_2, \ldots, \ell_s) \quad \text{en} \quad (S_n, \circ).$$

En otras palabras, el orden de una permutación es el mínimo común múltiplo de las longitudes de los ciclos en los que descompone.

Demostración. Escribimos $m := \text{m.c.m.}\,(\ell_1, \ell_2, \ldots, \ell_s)$. En primer lugar, veamos que $O(\sigma) \mid m$. Como los ciclos disjuntos conmutan, se cumple que

$$\sigma^m = (\sigma_1 \sigma_2 \cdots \sigma_s)^m = (\sigma_1 \sigma_2 \cdots \sigma_s) \cdots (\text{m veces}) \cdots (\sigma_1 \sigma_2 \cdots \sigma_s) = \sigma_1^m \sigma_2^m \cdots \sigma_s^m.$$

Como $\ell_i \mid m$ para todo $i \in \{1, 2, \ldots, s\}$, se tiene que existe $k_i \in \mathbb{N}_{\geq 1}$ tal que $\ell_i k_i = m$ y como $\sigma_i^{\ell_i} = \mathrm{Id}$, deducimos que $\sigma_i^m = \mathrm{Id}$ y que $\sigma^m = \mathrm{Id}$. Por consiguiente, como $\#S_n < \infty$, tenemos que $O(\sigma)$ es finito y podemos aplicar la Propiedad I.3.13.(III) para deducir que $O(\sigma) \mid m$.

Veamos que $m \mid O(\sigma)$. Sea $t := O(\sigma)$, luego $\sigma^t = \mathrm{Id}$. Como los ciclos disjuntos conmutan, se cumple que

$$\mathrm{Id} = \sigma^t = (\sigma_1 \sigma_2 \cdots \sigma_s)^t = \sigma_1^t \sigma_2^t \cdots \sigma_s^t.$$

Para cada $k \in \{1, 2, \ldots, n\}$ que σ_1 **deja fijo** se tiene que $\sigma_1(k) = k$ y que $\sigma_1^t(k) = k$.
Para cada $k \in \{1, 2, \ldots, n\}$ que σ_1 **no deja fijo**, como los ciclos son disjuntos, tenemos que $\sigma_i(k) = k$ para todo $i \in \{2, 3, \ldots, s\}$. En consecuencia, $k = \mathrm{Id}(k) = \sigma^t(k) = \sigma_1^t(k)$.
En resumen, para todo $k \in \{1, 2, \ldots, n\}$ se tiene que $\sigma_1^t(k) = k$, es decir, $\sigma_1^t = \mathrm{Id}$ y $\mathrm{Id} = \sigma_2^t \cdots \sigma_s^t$.
Por la Propiedad I.3.13.(III), concluimos que $O(\sigma_1) \mid t$ o, escrito de otro modo, $\ell_1 \mid t$.
Realizando el mismo procedimiento con los ciclos restantes vemos que $\ell_i \mid t$ para todo $i \in \{1, 2, \ldots, s\}$. Por la definición del mínimo común múltiplo, podemos asegurar que $m \mid t$, es decir, $m \mid O(\sigma)$. Finalmente, como $O(\sigma) \mid m$ y como $m \mid O(\sigma)$, concluimos que $O(\sigma) = m$ (ver Observación A.2.2). ■

El potencial de este Corolario se muestra en el siguiente ejemplo donde vemos como calcular los posibles ordenes de una permutación de un modo sencillo.

Ejemplo I.4.16 En S_7 tenemos $7! = 5040$ para determinar los posibles ordenes de todos los elementos solo tenemos que considerar las posibles descomposiciones en ciclos. Denotamos por $(-\ell-)$ un ciclo de longitud $\ell \in \mathbb{N}_{\geq 1}$ y sabemos que $\ell \geq 2$ (los ciclos de longitud 1 no tienen sentido). Tenemos las siguientes opciones $\sigma = \mathrm{Id}$ o:

Descomposición de σ	$O(\sigma)$	Descomposición de σ	$O(\sigma)$
$(-7-)$	7	$(-3-)(-3-)$	3
$(-6-)$	6	$(-3-)(-2-)(-2-)$	6
$(-5-)(-2-)$	10	$(-3-)(-2-)$	6
$(-5-)$	5	$(-3-)$	3
$(-4-)(-3-)$	12	$(-2-)(-2-)(-2-)$	2
$(-4-)(-2-)$	4	$(-2-)(-2-)$	2
$(-4-)$	4	$(-2-)$	2

Por consiguiente, si $\sigma \in S_n$, entonces $O(\sigma) \in \{1,2,3,4,5,6,7,10,12\}$.

Podemos dar un paso más y expresar toda permutación como composición de los ciclos más sencillos que existen las transposiciones. Como contrapartida, esta descomposición, a diferencia de la descomposición en ciclos, no es única y las transposiciones no necesariamente disjuntas.

Teorema I.4.17 Toda permutación de S_n, con $n \geq 2$, se puede expresar como composición de transposiciones (no necesariamente disjuntas ni únicas).

Demostración. Si $\sigma = \mathrm{Id}$ basta tomar $a,b \in \{1,2,\ldots,n\}$ con $a \neq b$ y comprobar que se cumple que $\sigma = (a,b)(b,a)$.
Si $\sigma \neq \mathrm{Id}$, por el Teorema I.4.12, basta comprobar que todo ciclo (no trivial) descompone como producto de transposiciones. Consideramos el ciclo $(i_1,\ i_2,\ \ldots, i_r)$ de longitud $r \in \mathbb{N}_{\geq 2}$, y comprobamos que

$$(i_1,\ i_2,\ \ldots, i_{r-1}, i_r) = (i_1,i_r)(i_1,i_{r-1})\cdots(i_1,i_3)(i_1,i_2).$$

¡Ojo! También podemos escribir: $(i_1,\ i_2,\ \ldots, i_{r-1}, i_r) = (i_2,i_1)(i_2,i_r)\cdots(i_2,i_4)(i_2,i_3)$ o también $(i_1,\ i_2,\ \ldots, i_{r-1}, i_r) = (i_r,i_{r-1})(i_r,i_{r-2})\cdots(i_r,i_2)(i_r,i_1)$. ■

Ejemplos I.4.18 En S_{10} consideramos el ciclo $(3,5,7,9)$ observamos que puede descomponer como producto de transposiciones de muchas formas distintas:

$$(3,5,7,9) = (3,9)(3,7)(3,5), \qquad (3,5,7,9) = (5,3)(5,9)(5,7),$$
$$(3,5,7,9) = (7,5)(7,3)(7,9), \qquad (3,5,7,9) = (9,7)(9,5)(9,3),$$
$$(3,5,7,9) = (1,2)(2,1)(3,9)(3,7)(3,5), \qquad (3,5,7,9) = (1,6)(3,9)(6,1)(4,8)(4,8)(3,7)(3,5).$$

Aunque el número de transposiciones en que se descompone una permutación no es único, lo que si se conserva siempre es su paridad, es decir, o siempre descompone en un número par de transposiciones o siempre descompone en un número impar de transposiciones. Para probar esta afirmación usaremos el siguiente Lema Auxiliar.

Lema I.4.19 La identidad sólo descompone como un número par de transposiciones, es decir, si $\mathrm{Id} = \tau_1\tau_2\cdots\tau_r$ con τ_k transposición para cada $k \in \{1,\ldots,r\}$, entonces r es par.

Demostración. En primer lugar, observamos que $r > 1$ porque $\mathrm{Id} \neq (i,j)$ para todos $i,j \in \{1,2,\ldots,n\}$. Por otro lado, si $r = 2$, entonces se cumple el lema.

Razonemos por inducción y asumimos que el lema se cumple para todo $s < r$, es decir, que:

Si $s < r$ y $\mathrm{Id} = \tau_1\tau_2\cdots\tau_s$ con τ_ℓ transposición para cada $\ell \in \{1,\dots,s\}$, entonces s es par.

Supongamos que $\mathrm{Id} = \tau_1\tau_2\cdots\tau_{r-1}\tau_r$ con τ_ℓ transposición para cada $\ell \in \{1,\dots,r\}$. Por tanto, $\tau_r = (i,j)$ para algún par de elementos $i,j \in \{1,2,\dots,n\}$ y tenemos las siguientes posibilidades para el producto $\tau_{r-1}\tau_r$:

(a) Si $\tau_{r-1}\tau_r = (i,j)(i,j)$, entonces $\tau_{r-1}\tau_r = \mathrm{Id}$.
(b) Si $\tau_{r-1}\tau_r = (i,k)(i,j)$ con $k \notin \{i,j\}$, entonces $\tau_{r-1}\tau_r = (i,j)(j,k)$.
(c) Si $\tau_{r-1}\tau_r = (j,k)(i,j)$ con $k \notin \{i,j\}$, entonces $\tau_{r-1}\tau_r = (i,k)(j,k)$.
(d) Si $\tau_{r-1}\tau_r = (m,k)(i,j)$ con $m,k \notin \{i,j\}$, entonces $\tau_{r-1}\tau_r = (i,j)(m,k)$.

En el caso (a) tenemos que $\mathrm{Id} = \tau_1\tau_2\cdots\tau_{r-2}\tau_{r-1}\tau_r = \mathrm{Id} = \tau_1\tau_2\cdots\tau_{r-2}$ y como $r-2 < r$, por hipótesis de inducción $r-2$ es par, luego r es par y hemos terminado.

En los caos (b), (c), (d) se sustituye $\tau_{r-1}\tau_r$ por $\widetilde{\tau_{r-1}}\widetilde{\tau_r}$ donde el elemento i no aparece en la transposición $\tilde{\tau}_r$. Repetimos el proceso para $\tau_{r-2}\widetilde{\tau_{r-1}}$. Si $\tau_{r-2}\widetilde{\tau_{r-1}} = \mathrm{Id}$, entonces $\mathrm{Id} = \tau_1\tau_2\cdots\tau_{r-3}\widetilde{\tau_r}$ y concluimos por hipótesis de inducción que $r-3+1$ es par, luego r es par. Si $\tau_{r-2}\widetilde{\tau_{r-1}} \neq \mathrm{Id}$, escribimos como antes $\mathrm{Id} = \tau_1\tau_2\cdots\widetilde{\widetilde{\tau_{r-2}}}\,\widetilde{\widetilde{\tau_{r-1}}}\,\widetilde{\widetilde{\tau_r}}$, donde las transposiciones $\widetilde{\widetilde{\tau_{r-2}}}$, $\widetilde{\widetilde{\tau_{r-1}}}$, $\widetilde{\widetilde{\tau_r}}$ no mueven a i. Iterando el razonamiento, debemos tener en algún momento que la composición de dos transposiciones consecutivas es la identidad, porque en caso contrario podríamos conseguir una descomposición de la identidad donde sólo la primera transposición mueve a i, luego i no quedaría fijo lo que es absurdo porque la identidad deja fijo a todos los elementos.

Como en algún momento el producto de dos transposiciones consecutivas es la identidad, obtenemos una descomposición de la identidad como un producto de $r-2$ transposiciones por hipótesis de inducción que $r-2$ es par, luego r es par. En consecuencia, por el Principio de Inducción Completa queda demostrado el lema. ■

Teorema I.4.20 Sea $\sigma \in S_n$ una permutación y $\tau_1,\dots,\tau_r,\tilde{\tau}_1,\dots,\tilde{\tau}_s \in S_n$ transposiciones. Si se cumple que

$$\sigma = \tau_1\tau_2\cdots\tau_r = \tilde{\tau}_1\tilde{\tau}_2\cdots\tilde{\tau}_s,$$

Entonces r y s tienen la misma paridad, o ambos números son pares o ambos son impares.

Demostración. Si $\sigma = \tau_1\tau_2\cdots\tau_r = \tilde{\tau}_1\tilde{\tau}_2\cdots\tilde{\tau}_s$, entonces tenemos que

$$\mathrm{Id} = (\tau_1\tau_2\cdots\tau_r)(\tilde{\tau}_1\tilde{\tau}_2\cdots\tilde{\tau}_s)^{-1} = \tau_1\tau_2\cdots\tau_r(\tilde{\tau}_s)^{-1}\cdots(\tilde{\tau}_2)^{-1}(\tilde{\tau}_1)^{-1}.$$

Como la inversa de una transposición es una transposición, por el Lema auxiliar I.4.19, deducimos que $r+s$ es par, luego r y s tiene la misma paridad. ■

Por consiguiente, podemos hablar de permutaciones pares e impares y asociar a toda permutación un índice.

Definición I.4.21 Sea $\sigma \in S_n$ una permutación. Si σ descompone en un número par de transposiciones, decimos que σ es una **permutación par** y si σ descompone en un número impar de transposiciones, decimos que σ es una **permutación impar**.
Definimos el índice de una permutación como:

$$i(\sigma) = \begin{cases} 1 & \text{si } \sigma \text{ es par} \\ -1 & \text{si } \sigma \text{ es impar} \end{cases}$$

Ejercicio I.4.22 ¿Qué elementos deja fijo el ciclo $(1,2,4)$?

Ejercicio I.4.23 (Subgrupo Alternado). Consideramos $A_n = \{\sigma \in S_n \ : \ \sigma \text{ es par}\}$ el conjunto de permutaciones pares, es decir, que descomponen como un número par de transposiciones. Probar que A_n es un subgrupo de $(S_n, \circ)$ de orden $n!/2$. Este subgrupo se denomina **grupo alternado de orden** n.

Ejercicio I.4.24 Probar que S_n no es abeliano cuando $n \geq 3$.

Ejercicio I.4.25 Probar que $H = \{\sigma \in S_5 : \sigma(1) = 1 \,\text{y}\, \sigma(3) = 3\}$ es un subgrupo de S_5.

Ejercicio I.4.26 Se consideran en S_9 las permutaciones

$$\sigma_1 = (1,3,2,6)(4,8,5)(7,9) \qquad \sigma_2 = (1,5,4,7,9)(3,6,8).$$

Expresar, como producto de ciclos disjuntos,

$$\sigma_1\sigma_2, \quad \sigma_2^{-1}\sigma_1, \quad \sigma_1^{50}, \quad \sigma_1^{15}\sigma_2^6.$$

Ejercicio I.4.27 Sea $\alpha = (1,3,5,7,9,8,6)(2,4,10)$. ¿Cuál es el menor entero positivo tal que $\alpha^n = \alpha^{-5}$?

Ejercicio I.4.28 Encontrar $\alpha, \beta \in S_3$ tales que $O(\alpha) = O(\beta) = 2$ y $O(\alpha\beta) = 3$. Encontrar $\alpha, \beta \in S_5$ tales que $O(\alpha\beta) = 5$ y $O(\alpha) = O(\beta) = 3$.

Ejercicio I.4.29 Si una permutación σ se expresa como producto de r ciclos disjuntos de longitudes respectivas $\ell_1 \leq \ell_2 \leq \cdots \leq \ell_r$ se dice que σ **es una permutación del tipo** $\{\ell_1, \ell_2, \ldots, \ell_r\}$.

(I) Determinar todos los tipos posibles de S_4.

(II) Determinar 10 tipos distintos para una permutación de orden 200 y calcular un valor n de forma que S_n contenga permutaciones de todos estos tipos.

(III) ¿Cuál es el menor valor de n para el cual existe en S_n un elemento de orden 200?

Ejercicio I.4.30 Calcular el número de elementos de orden 4 y 5 que hay en S_6 y A_6. (ver Ejercicio I.4.23).

Ejercicio I.4.31 Determinar todos los valores de n para los cuales S_n contiene algún elemento de orden 75.

Ejercicio I.4.32 Probar que para cualquier subgrupo H de S_n se cumple que $H \subseteq A_n$ o exactamente la mitad de los elementos de H son permutaciones pares (ver Ejercicio I.4.23).

Ejercicio I.4.33 Probar que una permutación que tiene orden impar, debe ser par. Deducir que si $(i_1, i_2, \ldots, i_\ell)$ es un ciclo de longitud ℓ, es par si ℓ es impar y es impar si ℓ es par.

Ejercicio I.4.34 (Permutaciones conjugadas). Se dice que dos permutaciones $\sigma_1, \sigma_2 \in S_n$ son **conjugadas** cuando existe $\tau \in S_n$ tal que $\sigma_2 = \tau\sigma_1\tau^{-1}$. Probar que:

(I) Si $\sigma = (i_1, i_2, \ldots, i_r) \in S_n$ y $\tau \in S_n$, entonces $\tau\sigma\tau^{-1} = (\tau(i_1), \tau(i_2), \ldots, \tau(i_r))$.

(II) Dos permutaciones son conjugadas si y sólo si son del mismo tipo, es decir, se descomponen en igual número de ciclos disjuntos de la misma longitud.

Ejercicio I.4.35 (Grupo Diédrico como grupo de permutaciones). El grupo diédrico (ver Ejercicio I.1.8) puede interpretarse también como el conjunto de las permutaciones de los vértices, numerados de 1 a n, de un polígono de n lados que conservan la adyacencia de los vértices. En concreto, D_n puede definirse también como el subgrupo de S_n generado por

$$r = (1\,2\,3\,4\,\ldots\,n) \quad \text{y} \quad s = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix} = \prod_{i=2}^{\lfloor \frac{n+1}{2} \rfloor} (i, n+2-i),$$

donde r se corresponde con el giro de centro el centro del polígono y ángulo $2\pi/n$ y s es la simetría cuyo eje pasa por el centro y el vértice 1. Para cada $n \geq 3$, probar que:

(I) $O(r) = n$ y $O(s) = 2$.
(II) $sr = r^{-1}s$ y deducir que $sr = r^{n-1}s$ y que $sr^k = r^{n-k}s$ para cada $k \in \mathbb{N}_{\geq 1}$.
(III) todo elemento de $< \{r,s\} >$ puede ponerse de la forma $r^j s^i$ con $j \in \{0,1,\ldots,n-1\}$ e $i \in \{0,1\}$.
(IV) el orden de $< \{r,s\} >$ es $2n$.

I.5 Clases Laterales. Subgrupos Normales. Grupo cociente

I.5.1 Clases laterales. Teorema de Lagrange

Definición I.5.1 Sea $(G,\cdot)$ un grupo y sea $S \subseteq G$ un subgrupo. Consideramos las dos relaciones siguientes:

($\mathbf{R_i}$) Relación de congruencia a la izquierda módulo S:
para todos $a,b \in G$ escribimos $a\,R_i\,b$ si $b^{-1}a \in S$.
En este caso, decimos que a está relacionado a la izquierda módulo S con b.

($\mathbf{R_d}$) Relación de congruencia a la derecha módulo S:
para todos $a,b \in G$ escribimos $a\,R_d\,b$ si $ab^{-1} \in S$.
En este caso, decimos que a está relacionado a la derecha módulo S con b.

Observación I.5.2 Si G es abeliano ambas relaciones coinciden.

Teorema I.5.3 Sea $(G,\cdot)$ un grupo y sea $S \subseteq G$ un subgrupo. Se cumple que:

(I) R_i y R_d son relaciones de equivalencia.

(II) La clase de equivalencia de un elemento $a \in G$ para R_i es:

$$[a]_{R_i} = aS := \{ax : x \in S\} \qquad (\textbf{Clase a la izquierda módulo S}).$$

(III) La clase de equivalencia de un elemento $a \in G$ para R_d es:

$$[a]_{R_d} = Sa := \{xa : x \in S\} \qquad (\textbf{Clase a la derecha módulo S}).$$

Demostración. Probaremos el teorema para R_i (Análogo para R_d).
Vemos que R_i es una relación de equivalencia, es decir, reflexiva, simétrica y transitiva.

- **Reflexiva.** Si $a \in G$, por (G.III), $a^{-1}a = 1_G$. Como S es subgrupo $1_G \in S$, luego $a^{-1}a = 1_G \in S$, es decir, $aR_i a$.
- **Simétrica.** Si $aR_i b$, entonces $b^{-1}a \in S$. Como S es subgrupo, tenemos que $(b^{-1}a)^{-1} \in S$. De acuerdo con el Ejercicio I.1.11, $(b^{-1}a)^{-1} = a^{-1}b$, luego $a^{-1}b \in S$, es decir, $bR_i a$.

- **Transitiva.** Si aR_ib y bR_ic, entonces $b^{-1}a \in S$ y $c^{-1}b \in S$. Por tanto, operando vemos que $c^{-1}a = c^{-1}bb^{-1}a \in S$ porque S es subgrupo, es decir, aR_ic

La clase de equivalencia de un elemento $a \in G$ para R_i es por definición:

$$[a]_{R_i} = \{b \in G : aR_ib\} = \{b \in G : b^{-1}a \in S\} = \{b \in G : b^{-1}a = s, s \in S\}.$$

Finalmente, operando vemos que:

$$[a]_{R_i} = \{b \in G : a = bs, s \in S\} = \{b \in G : as^{-1} = b, s \in S\}$$
$$\overset{\substack{S \text{ subgrupo} \\ s\in S \Leftrightarrow s^{-1}\in S}}{=} \{b \in G : ax = b, x \in S\} = \{ax : x \in S\} = aS. \qquad \blacksquare$$

Notación I.5.4 Del mismo modo que se describió en la Notación I.1.4, dada la relevancia de esta noción resulta conveniente transcribir el concepto de clase lateral para grupos con notación aditiva.

	Notación multiplicativa $(G,\cdot)$	**Notación aditiva** $(G,+)$
aR_ib	$b^{-1}a \in S$	$(-b)+a \in S$
aR_db	$ab^{-1} \in S$	$a+(-b) \in S$
$[a]_{R_i}$	$aS = \{ax : x \in S\}$	$a+S = \{a+x : x \in S\}$
$[a]_{R_d}$	$Sa = \{xa : x \in S\}$	$S+a = \{x+a : x \in S\}$

Habitualmente, cuando se emplea la notación aditiva el grupo es abeliano y, en ese caso, sabemos que ambas relaciones coinciden.

Ejemplo I.5.5 Calcular las clases laterales a la izquierda módulo $S = 6\mathbb{Z}$ en $(\mathbb{Z},+)$. Como $(\mathbb{Z},+)$ es abeliano las clases a izquierda y derecha coinciden y por el teorema anterior, para todo $a \in \mathbb{Z}$, se tiene que $[a]_{R_i} = a+6\mathbb{Z} = \{a+x : x \in 6\mathbb{Z}\}$.
De este modo, comprobamos que sólo hay seis clases posibles:

$$[0]_{R_i} = 0+6\mathbb{Z} = \{\dots,-12,-6,0,6,12,\dots\}, \qquad [3]_{R_i} = 3+6\mathbb{Z} = \{\dots,-9,-3,3,9,15,\dots\},$$
$$[1]_{R_i} = 1+6\mathbb{Z} = \{\dots,-11,-5,1,7,13,\dots\}, \qquad [4]_{R_i} = 4+6\mathbb{Z} = \{\dots,-8,-2,4,10,16,\dots\},$$
$$[2]_{R_i} = 2+6\mathbb{Z} = \{\dots,-10,-4,2,8,14,\dots\}, \qquad [5]_{R_i} = 5+6\mathbb{Z} = \{\dots,-7,-1,5,11,17,\dots\},$$

Observación I.5.6 En general, una clase a la izquierda no tiene que ser una clase a la derecha.

Ejemplo I.5.7 En D_3 (ver Ejercicio I.1.8) denotamos por a al giro de centro el centro del triángulo equilátero y ángulo $2\pi/3$ y b_i es la simetría cuyo eje pasa por el centro y el vértice i. Con la notación en términos de permutaciones (ver Ejercicio I.4.35) tenemos que $a = r = (123)$, $b_1 = s = (23)$, $b_2 = r^2s = (13)$ y $b_3 = rs = (12)$.
Calculamos la tabla multiplicativa:

$\cdot$	Id	a	a^2	b_1	b_2	b_3
Id	Id	a	a^2	b_1	b_2	b_3
a	a	a^2	Id	b_3	b_1	b_2
a^2	a^2	Id	a	b_2	b_3	b_1
b_1	b_1	b_2	b_3	Id	a	a^2
b_2	b_2	b_3	b_1	a^2	Id	a
b_3	b_3	b_1	b_2	a	a^2	Id

Consideramos el subgrupo $S_1 =< b_1 >= \{\mathrm{Id}, b_1\}$ y calculamos las clases laterales a izquierda y a derecha módulo S_1 y vemos que

$$\begin{array}{l|l} [\mathrm{Id}]_{R_i} = \mathrm{Id}S_1 = \{\mathrm{Id}, b_1\} = [b_1]_{R_i} & [\mathrm{Id}]_{R_d} = S_1\mathrm{Id} = \{\mathrm{Id}, b_1\} = [b_1]_{R_d} \\ [a]_{R_i} = aS_1 = \{a, b_3\} = [b_3]_{R_i} & [a]_{R_d} = S_1a = \{a, b_2\} = [b_2]_{R_d} \\ [a^2]_{R_i} = a^2S_1 = \{a^2, b_2\} = [b_2]_{R_i} & [a^2]_{R_d} = S_1a^2 = \{a^2, b_3\} = [b_3]_{R_d} \end{array}$$

Observamos que las clases a izquierda y derecha no coinciden $[a]_{R_i} \neq [a]_{R_d}$ y $[a^2]_{R_i} \neq [a^2]_{R_d}$

Propiedades I.5.8 — Clases laterales. Sea $(G, \bullet)$ un grupo y sea $S \subseteq G$ un subgrupo. Se cumple que:

(I) $G = \cup_{a\in G} aS = \cup_{a\in G} Sa$.

(II) para todos $a, b \in G$ se tiene que o bien $aS \cap bS = \emptyset$ o bien $aS = bS$.
para todos $a, b \in G$ se tiene que o bien $Sa \cap Sb = \emptyset$ o bien $Sa = Sb$.

(III) para todos $a, b \in G$ tenemos que:

$$\begin{array}{lllll} aS = bS & \Leftrightarrow & aR_i b & \Leftrightarrow & b^{-1}a \in S, \\ Sa = Sb & \Leftrightarrow & aR_d b & \Leftrightarrow & ab^{-1} \in S. \end{array}$$

(IV) para todo $a \in G$ se tiene que aS, S y Sa tienen el mismo cardinal.

(V) si $\mathfrak{D} = \{Sa : a \in G\}$ es el conjunto de clases a la derecha e $\mathfrak{I} = \{aS : a \in G\}$ es el conjunto de clases a la izquierda módulo S, entonces el cardinal de $\mathfrak{D}$ coincide con el cardinal de $\mathfrak{I}$.

Demostración. Por el Teorema I.5.3 sabemos que R_i y R_d son relaciones de equivalencia y que para todo $a \in G$ se cumple que $[a]_{R_i} = aS$ y que $[a]_{R_d} = Sa$, luego las propiedades (I), (II) y (III) se deducen propiedades de que satisfacen las clases de equivalencia definidas por cualquier relación de equivalencia: el conjunto total es igual a la unión de las clases, las clases o son disjuntas o son coincidentes y dos elementos están relacionados si y solo si su clase es la misma.

(IV) Basta comprobar que las aplicaciones:

$$\begin{array}{rccc} f_i: & S & \to & aS \\ & s & \to & as \end{array} \qquad \begin{array}{rccc} f_d: & S & \to & Sa \\ & s & \to & sa \end{array}$$

son biyectivas. Se tiene que f_i es inyectiva, porque si $f_i(s_1) = f_i(s_2)$, entonces $as_1 = as_2$ y multiplicando por a^{-1} vemos que $s_1 = s_2$. Se cumple que f_i es sobreyectiva, porque dado $x \in aS$, por definición, existe $s \in S$ tal que $x = as$, luego $f_i(s) = as = x$. (Análogo para f_d).

(V) Consideramos la aplicación

$$\begin{array}{rccc} \Phi: & \mathfrak{D} & \to & \mathfrak{I} \\ & Sa & \to & a^{-1}S \end{array}$$

Como Φ está definida sobre un conjunto de clases de equivalencia hay que comprobar que está **bien definida**, dados $a, b \in G$, en la misma clase a la derecha, se tiene que

$$Sa = Sb \overset{\text{(III)}}{\Rightarrow} ab^{-1} \in S \overset{a=(a^{-1})^{-1}}{\Rightarrow} (a^{-1})^{-1}b^{-1} \in S \overset{\text{(III)}}{\Rightarrow} a^{-1}S = b^{-1}S \Rightarrow \Phi(Sa) = \Phi(Sb).$$

Veamos que Φ es biyectiva:

- **Inyectiva.** Si $\Phi(Sa) = \Phi(Sb)$, tenemos que $a^{-1}S = b^{-1}S$ y, por (III), $(a^{-1})^{-1}b^{-1} \in S$, luego $ab^{-1} \in S$. De nuevo por (III), se tiene que $Sa = Sb$.
- **Sobreyectiva.** Dada $aS \in \mathfrak{I}$, basta observar que $\Phi(Sa^{-1}) = aS$.

En consecuencia, como Φ es una biyección, $\mathfrak{D}$ y $\mathfrak{I}$ tienen el mismo cardinal. ■

Definición I.5.9 Sean $(G,\cdot)$ un grupo y $S \subseteq G$ un subgrupo. Se define el **índice de S en G** como el cardinal de $\mathfrak{D}$ (o de $\mathfrak{I}$ porque coinciden por la Propiedad I.5.8.(V)) y se representa por $\#(G:S)$.

Teorema I.5.10 (Teorema de Lagrange). Sean $(G,\cdot)$ un grupo finito y $S \subseteq G$ un subgrupo. Se cumple que:

$$\#G = \#(G:S)\#S.$$

En consecuencia, el orden de cada subgrupo S de G divide al orden de G.

Demostración. Como G es finito tenemos que $\#(G:S) = r \in \mathbb{N}_{\geq 1}$ es finito. Elegimos un representante de cada una de las clases a la derecha módulo S, es decir, $a_i \in G$ para $i \in \{1,\dots,r\}$ de modo que $\mathfrak{D} = \{Sa_1, Sa_2, \dots Sa_r\}$ y que $Sa_j \cap Sa_i = \emptyset$ si $i \neq j$. Empleando las Propiedades I.5.8, vemos que

$$\#G \overset{(I)}{=} \sum_{j=1}^{r} \#(Sa_j) \overset{(IV)}{=} \sum_{j=1}^{r} \#(S) = r\,\#S = \#(G:S)\,\#S.$$

Dado un subgrupo $S \subseteq G$, directamente de la fórmula deducimos que $\#S \mid \#G$. ■

Observación I.5.11 El Teorema de Lagrange extiende la Propiedad I.3.16.(III) que conocíamos para *grupos cíclicos finitos* a todos los *grupos finitos*. Sin embargo, el recíproco, que hemos visto que es cierto para grupos cíclicos finitos (Propiedad I.3.16.(IV)), en general, no es cierto para grupos finitos cualesquiera. En otras palabras, el Teorema de Lagrange **no asegura que dado un divisor d de $\#G$ exista un subgrupo de orden d, de hecho, en general dicho subgrupo puede no existir** como muestra el Ejemplo I.5.12.

Ejemplo I.5.12 Consideramos el grupo A_4 alternado de orden 4, ver Ejercicio I.4.23, es decir, el grupo de las permutaciones pares de 4 elementos. Sabemos que $\#(A_4) = 4!/2 = 24/2 = 12$, vamos a probar que no posee ningún subgrupo de orden 6.

Razonamos por reducción al absurdo, supongamos que existe $H \subseteq A_4$ con $\#H = 6$. Observamos que los ciclos de orden 3 están en A_4 porque descomponen como producto de dos transposiciones:

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

Además observamos que en A_4 hay por lo menos 8 elementos de orden 3 (En realidad son exactamente 8). Por otro lado, por el Teorema de Lagrange $\#(A_4:H) = \#(A_4)/\#(H) = 12/6 = 2$, luego si a es un elemento de A_4 entre las clases H, aH y a^2H dos clases deben coincidir. En particular si a tiene orden 3 tenemos que $a^{-1} = a^2$ y vemos que

$$\text{Si } H = aH \;\Rightarrow\; (\mathrm{Id})^{-1}a \in H \Rightarrow a \in H.$$
$$\text{Si } H = a^2H \;\Rightarrow\; (\mathrm{Id})^{-1}a^2 \in H \Rightarrow a^2 \in H \;\Rightarrow\; a^{-1} \in H \overset{H \text{ subgrupo}}{\Rightarrow} a \in H.$$
$$\text{Si } aH = a^2H \;\Rightarrow (a)^{-1}a^2 \in H \Rightarrow a \in H.$$

En conclusión, hemos probado que si $a \in A_4$ y a tiene orden 3 entonces $a \in H$, luego $\#H \geq 8$ contradiciendo que $\#H = 6$. Por tanto, en A_4 no ha subgrupos de orden 6 pese a que $6 \mid \#(A_4)$.

En el artículo A_4 *Definitely Has No Subgroup of Order Six!*, ver [1], se pueden leer diversas pruebas de este mismo resultado.

Como consecuencia del Teorema de Lagrange deducimos varios resultados fundamentales.

Corolario I.5.13 Sea $(G,\bullet)$ un grupo finito y sea $a \in G$. Se cumple que $O(a) \mid \#G$.

Demostración. Por el Teorema de Lagrange, tenemos que $\# < a > \mid \#G$ y por la Propiedad I.3.13.(II), tenemos que $O(a) = \# < a >$, luego $O(a) \mid G$. ■

Corolario I.5.14 Todo grupo de orden primo es cíclico.

Demostración. Dado $(G,\bullet)$ un grupo de orden p con $p \in \mathbb{N}_{\geq 1}$ primo. Como $p > 1$, existe $a \in G$ tal que $a \neq 1_G$. Por el Teorema de Lagrange, se tiene que $\# < a > \mid p$. Como p es primo, por la Proposición A.2.20, sus únicos divisores positivos son 1 y p. Como $a \neq 1_G$, deducimos que $\# < a > = p$, luego se cumple que $G = < a >$. ■

Corolario I.5.15 Sea $(G,\bullet)$ un grupo con más de un elemento. Se tiene que
G es de orden primo si y solo si sus únicos subgrupos son $\{1_G\}$ y G.

Demostración. Directo empleando el Teorema I.3.18 y el Corolario I.5.14. ■

Definición I.5.16 Sea X un conjunto y R una relación de equivalencia sobre X. Un subconjunto A de X es un **sistema completo de representantes para la relación** R si
para cada $x \in X$ existe un único $a \in A$ tal que aRx.
En otras palabras, si A contiene un único elemento de cada clase de X módulo R.

Ejemplo I.5.17 De acuerdo con lo descrito en los Ejemplos I.5.5 y I.5.7 tenemos que:

(1) Un sistema completo de representantes de $(\mathbb{Z},+)$ módulo $6\mathbb{Z}$ (a izquierda o derecha) es $\{0,1,2,3,4,5\}$, otro sistema completo de representantes es $\{6,7,2,-3,-8,65\}$. Por otro lado, $\{0,1,8,9\}$ no es un sistema completo de representantes porque no hay un representante de cada clase y $\{0,1,2,3,4,5,6\}$ no es un sistema completo de representantes porque hay dos representantes de una misma clase.

(2) Un sistema completo de representantes de D_3, tanto para la relación R_d y como R_i módulo $S_1 = < b_1 >$, es $\{\mathrm{Id}, a, a^2\}$. Sin embargo, $\{\mathrm{Id}, a, b_3\}$ es un sistema completo de representantes para R_d módulo S_1 pero ¡ojo! no es un sistema completo de representantes para R_i módulo S_1 porque $[a]_{R_i} = aS_1 = b_3S_1 = [b_3]_{R_i}$, es decir, hay dos representantes de la misma clase y no hay ningún representante de la clase $[a^2]_{R_i} = a^2S_1 = \{a^2, b_2\} = b_2S_1 = [a^2]_{R_i}$.

I.5.2 Subgrupos normales

Como veremos en la siguiente subsección, cuando el conjunto de clases de equivalencias a la izquierda o a la derecha módulo S coincide podemos **dotar a dicho conjunto de estructura de grupo**. Como se mostró en el Ejemplo I.5.7, esto no siempre ocurre. En este apartado, estudiaremos los subgrupos S para los cuales se tiene dicha coincidencia.

Definición I.5.18 Sean $(G,\bullet)$ un grupo y $H \subseteq G$ un subgrupo. Se dice que H es **normal** si
para todo $a \in G$ se cumple que $aH = Ha$.
En caso de cumplirse, escribimos $H \lhd G$.

Existen varias formulaciones equivalentes del concepto de normalidad como muestra el siguiente resultado.

Proposición I.5.19 — Caracterización de los subgrupos normales. Sean $(G,\bullet)$ un grupo y $H \subseteq G$ un subgrupo. Las siguientes condiciones son equivalentes:

(I) H es un subgrupo normal, es decir, para todo $a \in G$ se tiene que $aH = Ha$.

(II) las relaciones a la izquierda y a derecha módulo H coinciden, es decir, para todos $a,b \in G$ se tiene que $aR_i b$ si y solo si $aR_d b$.

(III) para todo $a \in G$ y para todo $h \in H$ tenemos que $aha^{-1} \in H$.

Demostración. (I) $\Rightarrow$ (II) Dados $a,b \in G$, tenemos que

$$aR_i b \overset{\text{Prop. I.5.8.(III)}}{\Leftrightarrow} aH = bH \overset{\text{(I)}}{\Leftrightarrow} Ha = Hb \overset{\text{Prop. I.5.8.(III)}}{\Leftrightarrow} aR_d b$$

(II) $\Rightarrow$ (III) Dados $a \in G$ y $h \in H$, veamos que $aha^{-1} \in H$. Como $h \in H$, tenemos que

$$1_G h = (a^{-1}a)h \in H.$$

Por tanto, por asociatividad, se cumple que $a^{-1}(ah) \in H$, es decir, $ahR_i a$ y, por (II), $ahR_d a$. Finalmente, deducimos que $aha^{-1} \in H$.

(III) $\Rightarrow$ (I) En primer lugar, dado $a \in H$, veamos que $aH \subseteq Ha$. Dado $b \in aH$, $b = ah$ para algún $h \in H$. Multiplicando por la derecha por a^{-1}, se tiene que $ba^{-1} = aha^{-1}$ para algún $h \in H$ y, por (III), $ba^{-1} \in H$. En consecuencia, $ba^{-1} = \tilde{h}$ para algún $\tilde{h} \in H$, es decir, $b = \tilde{h}a$ para algún $\tilde{h} \in H$, o equivalentemente $b \in Ha$.

Análogamente, vemos que $Ha \subseteq aH$ y concluimos que $aH = Ha$. ■

Observación I.5.20 Cualquier subgrupo de un grupo abeliano es normal porque las clases a izquierda y derecha coinciden (ver Observación I.5.6).

Ejemplo I.5.21 De acuerdo con lo descrito en los Ejemplos I.5.5 y I.5.7 tenemos que:

(1) Observamos que $6\mathbb{Z} \lhd \mathbb{Z}$, de hecho, como $(\mathbb{Z},+)$ es abeliano $n\mathbb{Z} \lhd \mathbb{Z}$ para todo $n \in \mathbb{N}_{\geq 1}$.

(2) Vemos que $< a >= \{\mathrm{Id}, a, a^2\}$ es normal en D_3 pero S_1 no es normal en D_3.

Proposición I.5.22 Sean $(G,\bullet)$ un grupo y $\{H_i\}_{i\in I}$ una familia de subgrupos normales de G. Se cumple que

$$\cap_{i\in I} H_i \qquad \text{es un subgrupo normal.}$$

Demostración. Por la Proposición I.2.6, sabemos que $\cap_{i\in I} H_i$ es un subgrupo. Dados $h \in \cap_{i\in I} H_i$ y $a \in G$ tenemos que $h \in H_i$ para todo $i \in I$. Como $H_i \lhd G$, por la Proposición I.5.19, $aha^{-1} \in H_i$ para todo $i \in I$ luego $aha^{-1} \in \cap_{i\in I} H_i$. De nuevo por la Proposición I.5.19, se tiene que $\cap_{i\in I} H_i \lhd G$. ■

Notación I.5.23 Dados dos subconjuntos A,B de $(G,\bullet)$, definimos el conjunto producto por:

$$AB = \{ab : a \in A, b \in B\}.$$

Observación I.5.24 Si H y K son subgrupos de $(G,\bullet)$, HK puede no ser un subgrupo.

Ejemplo I.5.25 En D_3, ver Ejemplo I.5.7, consideramos los subgrupos $S_1 =< b_1 >= \{\mathrm{Id}, b_1\}$ y $S_2 =< b_2 >= \{\mathrm{Id}, b_2\}$. Observamos que el conjunto $S_1S_2 = \{\mathrm{Id}, b_1, b_2, b_1b_2 = a\}$ no es un subgrupo porque $a^{-1} \notin S_1S_2$.

Lema I.5.26 Sean $(G,\cdot)$ un grupo y $H,K\subseteq G$ subgrupos. Se cumple que:

(I) si H y K son finitos, entonces $\#HK=\dfrac{\#H\,\#K}{\#(H\cap K)}$.

(II) HK es un subgrupo si y sólo si $HK=KH$.
En caso de ser cierto, se tiene que $<H\cup K>=HK=KH$.

Demostración. (I) Distinguimos tres etapas:

(a) Veamos que $\#K=\#(H\cap K)\,\#(K:H\cap K)$. Denotamos por $C:=H\cap K$, sabemos que es un subgrupo de G por ser intersección de subgrupos, como $C\subseteq K$, C es también un subgrupo de K, luego C es finito. De forma directa por el Teorema de Lagrange se tiene la igualdad.

(b) Además, denotamos por $n:=\#(K:C)=\#(K:H\cap K)$, luego hay exactamente n clases a la derecha módulo C en K . Elegimos un sistema completo de representantes $\{a_1,a_2,\dots,a_n\}$ de R_d módulo C en K, es decir, $a_i\in K$, para todo $k\in K$ existe a_i tal que $Ck=Ca_i$ y $Ca_i\neq Ca_j$ si $i\neq j$.

(c) Veamos que $Ha_i\cap Ha_j=\emptyset$ si $i\neq j$. Observamos que

$$Ha_i\cap Ha_j\neq\emptyset \overset{\text{Prop. I.5.8}}{\Leftrightarrow} Ha_i=Ha_j \overset{\text{Prop. I.5.8}}{\Leftrightarrow} a_ia_j^{-1}\in H \overset{a_i,a_j\in K,\ K\text{ Subgrupo}}{\Leftrightarrow} a_ia_j^{-1}\in H\cap K=C \overset{\text{Prop. I.5.8}}{\Leftrightarrow} Ca_i=Ca_j. \overset{\text{Prop. I.5.8}}{\Leftrightarrow} i=j$$

(d) Veamos que $HK=\cup_{i=1}^n Ha_i$. Tenemos que $Ha_i\subseteq HK$ para todo $i\in\{1,\dots,n\}$ porque $a_i\in K$, luego $\cup_{i=1}^n Ha_i\subseteq HK$. Por otra parte, dado $b\in HK$ existen $h\in H$ y $k\in K$ tales que $b=hk$. Como $\{a_1,a_2,\dots,a_n\}$ es un sistema completo de representantes existe $j\in\{1,\dots,n\}$ tal que $k\in Ca_j$, luego $k=ca_j$ con $c\in C=H\cap K$. Por consiguiente vemos que $b=hk=hca_j\in Ha_j$, luego $HK\subseteq\cup_{i=1}^n Ha_i$ y concluimos que $HK=\cup_{i=1}^n Ha_i$.

Empleando estas propiedades vemos que

$$\#(HK)\overset{(c),(d)}{=}\sum_{i=1}^n\#(Ha_i)\overset{\text{Prop. I.5.8}}{=}\sum_{i=1}^n\#H=n\#H\overset{(b)}{=}\#(K:H\cap K)\#H\overset{(a)}{=}\frac{\#K\#H}{\#(H\cap K)}$$

(II) En primer lugar, supongamos que HK es subgrupo. Dado $a\in HK$, como HK es subgrupo, $a^{-1}\in HK$, luego existen $h\in H$ y $k\in K$ tales que $a^{-1}=hk$. Por tanto, se tiene que

$$a=(a^{-1})^{-1}=(hk)^{-1}=k^{-1}h^{-1}\overset{\substack{k^{-1}\in K\\ h^{-1}\in H}}{\in}KH.$$

Por consiguiente, $HK\subseteq KH$ y, análogamente, se prueba que $KH\subseteq HK$.

Recíprocamente, supongamos que $HK=KH$. Vemos que $HK\neq\emptyset$ porque $H\subseteq HK$, dados $a_1,a_2\in HK$ existen $h_1,h_2\in H$ y $k_1,k_2\in K$ tales que $a_1=h_1k_1$ y $a_2=h_2k_2$. Observamos que

$$a_1a_2^{-1}=h_1k_1(h_2k_2)^{-1}=h_1\underbrace{k_1k_2^{-1}}_{k_3\in K}h_2^{-1}\overset{K\text{ subgrupo}}{=}\underbrace{h_1k_3}_{HK}h_2^{-1}\overset{HK=KH}{=}\underbrace{k_4h_4}_{k_4\in K,h_4\in H}h_2^{-1}\in KH=HK.$$

Por el Test de Caracterización de subgrupos, concluimos que HK es un subgrupo.

Como $<(H\cup K)>$ es un subgrupo que contiene a H y a K debe contener a todos los productos de elementos de H por elementos de K y de elementos de K por elementos de H. Por consiguiente, siempre se cumple que $HK,KH\subseteq<(H\cup K)>$. En caso de que HK sea subgrupo, como $H=H1_G\subseteq HK$ y como $K=1_GK\subseteq HK$, tendríamos que HK es un subgrupo

que contiene a $H \cup K$. Como $< (H \cup K) >$ es el subgrupo más pequeño con esta propiedad, se cumpliría que $< (H \cup K) > \subseteq HK$. En consecuencia, si HK es subgrupo o, equivalentemente, si $HK = KH$, entonces $< H \cup K > = HK = KH$. ■

Teorema I.5.27 Sean $(G, \cdot)$ un grupo, $N \lhd G$ y $S \subseteq G$ un subgrupo. Se tiene que:
(I) $N \cap S \lhd S$.
(II) $NS = SN$.
(III) NS es subgrupo de G y $N \lhd NS$.
(IV) si S y N son finitos, entonces $\#NS = \dfrac{\#N\,\#S}{\#(N \cap S)}$.

Demostración. (I) $N \cap S$ es subgrupo por ser intersección de subgrupos. Dados $h \in N \cap S$ y $s \in S$ tenemos que

$$\begin{cases} \text{Como } h \in N \text{ y } s \in G \text{ y } N \lhd G, \text{ por la Prop. I.5.19, se tiene que } shs^{-1} \in N \\ \text{Como } h, s \in S \text{ y } S \text{ es subgrupo, se tiene que } shs^{-1} \in S \end{cases}$$

Por consiguiente, vemos que $shs^{-1} \in N \cap S$ y, de nuevo por la Proposición I.5.19, $N \cap S \lhd S$.
(II) Dado $h \in NS$, tenemos que $h = ns$ con $n \in N$ y con $s \in S$, luego $h = ss^{-1}ns$. Como N es normal, $N \lhd G$, tenemos que $s^{-1}ns = \tilde{n} \in N$. En consecuencia, $h = s\tilde{n} \in SN$ y deducimos que $NS \subseteq SN$. Análogamente se prueba que $SN \subseteq NS$, luego $NS = SN$
(III) Por el Lema I.5.26.(II) y el apartado (II), tenemos que NS es subgrupo de G y, como $N \lhd G$, comprobamos de forma directa que $N \lhd NS$.
(IV) Directa por el Lema I.5.26.(I). ■

I.5.3 Grupo cociente

Teorema I.5.28 Sean $(G, \cdot)$ un grupo, $N \lhd G$ y G/N el conjunto de clases de equivalencia módulo N en G. Definimos la correspondencia:

$$\begin{array}{rccc} \cdot : & G/N \times G/N & \to & G/N \\ & (aN, bN) & \to & (ab)N \end{array}$$

Entonces $(G/N, \cdot)$ es un grupo y su orden es $\#(G : N)$.

Demostración. En primer lugar veamos que la operación binaria interna $\cdot$ está **bien definida**. Dados cualesquiera $a_1, a_2, b_1, b_2 \in G$, de modo que $a_1N = a_2N$ y que $b_1N = b_2N$, veamos que $(a_1b_1)N = (a_2b_2)N$. Observamos que

$$\begin{aligned} h \in (a_1b_1)N &\Leftrightarrow h = a_1b_1n_1 \text{ para algún } n_1 \in N \overset{b_1N=b_2N}{\Leftrightarrow} h = a_1b_2n_2 \text{ para algún } n_2 \in N \\ &\overset{\substack{\text{Como } N \lhd G \\ b_2N = Nb_2}}{\Leftrightarrow} h = a_1n_3b_2 \text{ para algún } n_3 \in N \overset{a_1N=a_2N}{\Leftrightarrow} h = a_2n_4b_2 \text{ para algún } n_4 \in N \\ &\overset{\substack{\text{Como } N \lhd G \\ b_2N = Nb_2}}{\Leftrightarrow} h = a_2b_2n_5 \text{ para algún } n_5 \in N \Leftrightarrow h \in (a_2b_2)N. \end{aligned}$$

Veamos que $(G/N, \cdot)$ es un grupo, es decir, satisface (G.I), (G.II) y (G.III). Dados $a, b, c \in G$ tenemos que

(G.I) **Asociativa:** $aN(bNcN) = aN(bc)N = (a(bc))N \overset{\substack{\text{(G.I)} \\ \text{en } G}}{=} ((ab)c)N = (ab)NcN = (aNbN)cN$.
(G.II) **Neutro:** 1_GN es el elemento neutro de G/N dado que

$$1_GNaN = (1_Ga)N = aN = (a1_G)N = aN1_GN.$$

(G.III) **Inverso:** $a^{-1}N$ es el inverso de aN porque

$$a^{-1}NaN = (a^{-1}a)N = 1_G N = (aa^{-1})N = aNa^{-1}N.$$

■

Observación I.5.29 Por la definición del producto en el grupo cociente, vemos de forma directa que el cociente de cualquier grupo abeliano es abeliano.

Como muestra de las aplicaciones del grupo cociente tenemos el siguiente resultado.

Teorema I.5.30 (Teorema de Cauchy para grupos abelianos). Sean $(G,\cdot)$ un grupo abeliano y finito y $p \in \mathbb{N}_{\geq 1}$, con p primo, tal que $p \mid \#G$. Entonces existe $a \in G$ con $O(a) = p$.

Demostración. Razonemos por inducción en $\#G$. Para cada $k \in \mathbb{N}_{\geq 2}$, consideramos

$$P(k) \ : \text{ para todo grupo } G \text{ con } \#G = k \text{ y } p \text{ primo con } p \mid \#G \quad \Rightarrow \quad \exists a \in G \text{ con } O(a) = p.$$

En primer lugar veamos que se cumple para $P(2)$. Si $\#G = 2$, por el Corolario I.5.14, G es cíclico, luego si p es primo y $p \mid \#G$, entonces $p = 2$. En consecuencia basta tomar a con $G =< a >$ porque $O(a) = \# < a >= \#G = 2$.

Asumimos que para un cierto $n > 2$ se cumple $P(k)$ para todo $k < n$ y supongamos que G es un grupo abeliano con $\#G = n$ y p es un primo con $p \mid n$. Como $\#G = n > 2$, existe $g \in G$ con $g \neq 1_G$, luego $O(g) = m > 1$. Por el Teorema Fundamental de la Aritmética, existe $q \in \mathbb{N}_{\geq 1}$, con q primo, tal que $q \mid m$. Por tanto, $m = qr$ y observamos que

$$O(g^r) = \frac{O(g)}{\text{m.c.d.}\,(m,r)} = \frac{m}{r} = q.$$

Si $q = p$ hemos terminado. Si $q \neq p$, como todo subgrupo de un grupo abeliano es normal, denotamos $N =< g^r >$ y construimos el grupo cociente $\tilde{G} = G/N$. Por la Observación I.5.29, tenemos que $\tilde{G}$ y vemos que

$$\#\tilde{G} = \#(G:N) = \frac{\#G}{\# < g^r >} = \frac{n}{q} < n.$$

Como p, q son primos con $p \neq q$ y con $p \mid n$ y $q \mid n$ tenemos que $p \mid (n/q) = \#\tilde{G}$, ver Corolario A.2.13.(IV). Por lo tanto, por **hipótesis de inducción**, existe $cN \in \tilde{G}$ con $O(cN) = p$. Observamos que

$$\text{Como } O(cN) = p > 1 \ \Rightarrow \ cN \neq N \ \Rightarrow \ c \notin N \ \Rightarrow \ c \neq 1_G.$$
$$\text{Como } O(cN) = p \ \Rightarrow \ (cN)^p = N \ \Rightarrow \ c^p N = N \ \Rightarrow \ c^p \in N.$$

Si $c^p = 1$, como $c \neq 1_G$, necesariamente $O(c) = p$ y hemos terminado. Si $c^p \neq 1$, probaremos que $O(c^q) = p$, con lo que se concluye la prueba. Como $c^p \in N$ y como $\#N = q$, entonces $c^{pq} = 1$, luego o bien $O(c) = p$ (imposible porque $c^p \neq 1$) o bien $O(c) = q$ o bien $O(c) = pq$. Si $O(c) = q$, tendríamos que $c^q = 1_G$, luego $(cN)^q = N$, lo que es imposible porque $O(cN) = p$ y p y q son primos distintos. Por ende, $O(c) = pq$ y vemos que

$$O(c^q) = \frac{O(c)}{\text{m.c.d.}\,(O(c),q)} = \frac{pq}{q} = p.$$

Consecuentemente, $P(n)$ es cierta y por el Principio de Inducción Completa queda demostrado el Teorema. ■

Ejercicio I.5.31 Sea $(G,\cdot)$ un grupo y sean S,T subgrupos de G con $S \subseteq T$. Probar que:

$$\#(G:S) = \#(G:T)\#(T:S).$$

Ejercicio I.5.32 Determinar las clases laterales (a izquierda y derecha) definidas en:
(I) $(4\mathbb{Z},+)$ por el subgrupo $S = 20\mathbb{Z}$.
(II) $(\mathbb{Z}/3\mathbb{Z},+)\times(\mathbb{Z}/6\mathbb{Z},+)$ por el subgrupo $S = \langle(1,2)\rangle$.
(III) $(\mathbb{Z}/4\mathbb{Z},+)\times(\mathbb{Z}/6\mathbb{Z},+)$ por el subgrupo $S = \langle(2,4)\rangle$.
(IV) $(S_4,\circ)$ por los subgrupos $S_1 = \langle(1\,2\,3)\rangle$, $S_2 = \langle(1\,2\,3\,4)\rangle$.

Ejercicio I.5.33 Determinar las clases a la izquierda de $S = \{1,(12)(34)\}$ en S_4, calculando antes las de S en $V_4 = \{1,(12)(34),(13)(24),(14)(23)\}$ y las de V_4 en S_4 (Emplear el Ejercicio I.5.31).
Demostrar que V_4 es un subgrupo normal de S_4 y describir (elementos y tabla) de S_4/V_4.

Ejercicio I.5.34 Si $(G,\cdot)$ es un grupo cíclico de orden 30, $G = \langle a\rangle$, determinar las clases que definen los subgrupos $S = \langle a^4\rangle$ y $T = \langle a^{12}\rangle$.

Ejercicio I.5.35 Probar que $(\mathbb{Q},+)$ no posee ningún subgrupo propio de índice finito.

Ejercicio I.5.36 Probar que todo subgrupo S de un grupo $(G,\cdot)$ que cumple que $\#(G:S) = 2$ es normal.

Ejercicio I.5.37 ¿Es $H = \langle(1234)\rangle$ normal en S_5?¿y en S_4?

Ejercicio I.5.38 Probar que el centro de un grupo $Z(G)$ es normal en G. Probar que el normalizador $N(S)$ de un subgrupo S de G es el subgrupo más grande en el que S es normal.

Ejercicio I.5.39 Probar que A_n es normal en S_n.

Ejercicio I.5.40 Probar que D_4 existen subgrupos H,K de forma que $H \lhd K$ y $K \lhd D_4$ y H no es normal en D_4.

Ejercicio I.5.41 Consideramos el subgrupo $S = \langle 4\rangle$ en el grupo $(\mathbb{Z}/12\mathbb{Z},+)$. Dar la lista de los elementos de $(\mathbb{Z}/12\mathbb{Z})/S$ y construir la tabla del grupo.

Ejercicio I.5.42 Probar que $S = \langle r^2\rangle$ es normal en D_4, determinar los elementos de D_4/S y construir la tabla del grupo cociente.

Ejercicio I.5.43 Probar que el cociente de cualquier grupo cíclico es cíclico.

Ejercicio I.5.44 Sea $(G,\cdot)$ un grupo de orden pq con p,q primos. Probar que cada subgrupo propio de G es cíclico.

Ejercicio I.5.45 Sea $(G,\cdot)$ un grupo de orden 155 y a,b dos elementos de G distintos del elemento neutro y tales que $O(a) \neq O(b)$. Probar que $G = \langle a,b\rangle$.

Ejercicio I.5.46 Calcular el orden del elemento $14+\langle 8\rangle$ en el grupo cociente $(\mathbb{Z}/24\mathbb{Z})/\langle 8\rangle$.

Ejercicio I.5.47 Determinar el orden del grupo $(\mathbb{Z}/4\mathbb{Z},+)\times(\mathbb{Z}/6\mathbb{Z},+)$ al hacer cociente por el subgrupo $\langle(2,2)\rangle$ ¿Es este grupo cíclico?

Ejercicio I.5.48 Probar que en un grupo de G/H puede ocurrir que $O(aH)=O(bH)$ con $O(a)\neq O(b)$.

Ejercicio I.5.49 Probar que si $(G,\cdot)$ es un grupo finito y S un subgrupo de G, entonces para cada $a\in G$ se cumple que $aSa^{-1}=\{asa^{-1}:s\in S\}$ es subgrupo de G con $\#(S)=\#(aSa^{-1})$.

Ejercicio I.5.50 (Acción de grupo). Dados X un conjunto no vacío cualquiera y $(G,\cdot)$ un grupo y $A:X\times G\to X$ una aplicación. Diremos que A es una **acción de G sobre X** si verifica las dos propiedades siguientes:

(A.I) Para todos $g_1,g_2\in G$ y todo $x\in X$ se tiene que $A(A(x,g_1),g_2)=A(x,g_1\cdot g_2)$.

(A.II) Para todo $x\in X$ se tiene que $A(x,1_G)=x$.

Dada una acción $A:X\times G\to X$ diremos que es **fiel** si se cumple que

Para todo $g\in G$, si $A(x,g)=x$ para todo $x\in X$, entonces $g=1_G$,

es decir, 1_G es el único elemento que cumple (A.II).
Dada una acción $A:X\times G\to X$ diremos que es **transitiva** si se cumple que

Para todos $x_1,x_2\in X$ existe $g\in G$ tal que $A(x_1,g)=x_2$

Si g es único se dice que A es **simplemente transitiva.** Se pide:

(I) Probar que $S=\{z\in\mathbb{C}:|z|=1\}$ es un subgrupo de $(\mathbb{C}\backslash\{0\},\cdot)$ y que la aplicación $A:\mathbb{C}\times S\to\mathbb{C}$ definida por $A(x,z)=xz$ es una acción de grupo. ¿Qué representa geométricamente? ¿Es fiel? ¿y transitiva?

(II) Sea V un $\mathbb{K}-$espacio vectorial. Probar que el producto por escalares de $\mathbb{K}\times V\to V$ es una acción de $(\mathbb{K}\backslash\{0_{\mathbb{K}}\},\cdot)$ sobre V. ¿Es fiel? ¿y transitiva?

Ejercicio I.5.51 (Órbita y estabilizador de una acción de grupo). Dados X un conjunto no vacío cualquiera y $(G,\cdot)$ un grupo y $A:X\times G\to X$ una acción de grupo. Se define el **estabilizador de $x\in X$ por A** mediante:

$$\mathrm{stab}_A(x)=\{g\in G\ :\ A(x,g)=x\}.$$

y la **órbita de x bajo la acción A** como:

$$\mathrm{orb}_A(x)=\{A(x,g)\ :\ g\in G\}.$$

Se pide:

(I) Probar que para todo $x\in X$ se tiene que $\mathrm{stab}_A(x)$ es un subgrupo de G.

(II) Si G es finito, probar que para todo $x\in X$ se tiene que $\#G=\#\mathrm{orb}_A(x)\cdot\#\mathrm{stab}_A(x)$.

(III) Si A es fiel, ¿qué podemos deducir de los estabilizadores?

(IV) Si A es transitiva, ¿qué podemos deducir de las órbitas? Si, además, G es finito, ¿qué sabemos de los estabilizadores?

(V) Consideramos el conjunto X de cartas de oros de la baraja española. Tenemos una máquina que reordena las cartas, si metemos las cartas ordenadas del 1 al 12 nos devuelve las cartas en el siguiente orden 2, 12, 3, 11, 4, 6, 10, 7, 5, 1. Describir el grupo G de permutaciones originado por la máquina. Calcular las órbitas y los estabilizadores de 1, 2, 4, 7 por la acción de G.

I.6 Homomorfismos de grupos

I.6.1 Nociones básicas

Definición I.6.1 Sean $(G,\bullet_G)$ y $(H,\bullet_H)$ dos grupos y $f: G \to H$ una aplicación. Decimos que f es un **homomorfismo de grupos** si para todos $a,b \in G$ se tiene que

$$f(a \bullet_G b) = f(a) \bullet_H f(b).$$

Definición I.6.2 Sean $(G,\bullet_G)$ y $(H,\bullet_H)$ dos grupos.

(A) Si $f: G \to H$ es un homomorfismo y, además, f es biyectivo, entonces decimos que f es un **isomorfismo**.

(B) Si existe un isomorfismo $f: G \to H$, entonces decimos que G y H son isomorfos y lo denotamos por $G \approx H$.

(C) Si $f: G \to G$ es un homomorfismo, entonces decimos que f es un **endomorfismo**.

(D) Si $f: G \to G$ es un isomorfismo, entonces decimos que f es un **automorfismo**.

Ejemplos I.6.3 (1) Entre dos grupos cualesquiera, la aplicación constante $f: G \to H$ dada para todo $a \in G$ por $f(a) = 1_H$ es un homomorfismo de grupos.

(2) Si $m \in \mathbb{Z}$, entonces las aplicaciones:

$$\begin{array}{rcl} f_m : (\mathbb{Z},+) & \to & (m\mathbb{Z},+) \\ n & \to & n \cdot m \end{array} \qquad \begin{array}{rcl} g_m : (\mathbb{Z},+) & \to & (\mathbb{Z}/m\mathbb{Z},+) \\ n & \to & n \,(\text{mód } m) \end{array}$$

son homomorfismos de grupos.

(3) Si G es un grupo, S es un subgrupo de G y N es un subgrupo normal de G, entonces la inclusión canónica i y la aplicación de paso al cociente p_N

$$\begin{array}{rcl} i : S & \to & G \\ s & \to & s \end{array} \qquad \begin{array}{rcl} p_N : G & \to & G/N \\ g & \to & gN \end{array}$$

son homomorfismos de grupos.

Propiedades I.6.4 — Homomorfismos de grupos. Sean $(G,\bullet)$ y $(H,\bullet)$ dos grupos y un homomorfismo de grupos $f: G \to H$. Se cumple que:

(I) $f(1_G) = 1_H$.

(II) para todo $a \in G$ se tiene que $f(a^{-1}) = (f(a))^{-1}$.

(III) Si S es un subgrupo de G, entonces $f(S)$ es un subgrupo de H.

(IV) Si T es un subgrupo de H, entonces $f^{-1}(T)$ es un subgrupo de G.

(V) Si T es un subgrupo normal de H, entonces $f^{-1}(T)$ es un subgrupo normal de G.

Demostración. (I) Como $1_G = 1_G \cdot 1_G$, tenemos que $f(1_G) = f(1_G \cdot 1_G) = f(1_G) \cdot f(1_G)$ $(\star)$. Por consiguiente, multiplicando a ambos lados por $(f(1_G))^{-1}$, se tiene que

$$1_H \overset{\text{(G.III)}}{=} (f(1_G))^{-1} f(1_G) \overset{(\star)}{=} (f(1_G))^{-1} \cdot (f(1_G) \cdot f(1_G)) \overset{\text{(G.I)+(G.III)}}{=} (1_H) \cdot f(1_G) \overset{\text{(G.II)}}{=} f(1_G).$$

(II) Veamos que $f(a^{-1})$ es el inverso de $f(a)$:

$$f(a^{-1}) \cdot f(a) \overset{f \text{ hom}}{=} f(a^{-1} \cdot a) \overset{\text{(G.III)}}{=} f(1_G) \overset{\text{(I)}}{=} 1_H.$$
$$f(a) \cdot f(a^{-1}) \overset{f \text{ hom}}{=} f(a \cdot a^{-1}) \overset{\text{(G.III)}}{=} f(1_G) \overset{\text{(I)}}{=} 1_H.$$

Por tanto, por la unicidad del elemento inverso $f(a^{-1}) = (f(a))^{-1}$.

(III) Como $1_G \in S$, tenemos que $1_H \in f(S)$, luego $f(S) \neq \emptyset$. Dados $x,y \in f(S)$ veamos que $x \cdot y^{-1} \in f(S)$. Como $x,y \in f(S)$ existen $a,b \in S$ tales que $f(a) = x$ y $f(b) = y$, entonces

$$x \cdot y^{-1} = f(a) \cdot (f(b))^{-1} \overset{\text{(II)}}{=} f(a)f(b^{-1}) \overset{f \text{ hom}}{=} f(ab^{-1}).$$

Como S es subgrupo, por el Test de Caracterización de Subgrupos $ab^{-1} \in S$, luego $x \cdot y^{-1} \in f(S)$ y, de nuevo por el Test de Caracterización de Subgrupos, concluimos que $f(S)$ es subgrupo.

(IV) Como $1_H \in T$, tenemos que $1_G \in f^{-1}(T)$, luego $f^{-1}(T) \neq \emptyset$. Dados $a,b \in f^{-1}(T)$ veamos que $a \cdot b^{-1} \in f^{-1}(T)$. Como $a,b \in f^{-1}(T)$, tenemos que $f(a), f(b) \in T$ y, como T es subgrupo, por el Test de Caracterización de Subgrupos $f(a)(f(b))^{-1} \in T$. Por (II), se tiene que $f(a)f(b^{-1}) \in T$ y, como f es homomorfismo, $f(ab^{-1}) \in T$, luego $ab^{-1} \in f^{-1}(T)$. En consecuencia, por el Test de Caracterización de Subgrupos, concluimos que $f^{-1}(T)$ es subgrupo.

(V) Dados $g \in G$ y $x \in f^{-1}(T)$ veamos que $gxg^{-1} \in f^{-1}(T)$. Observamos que

$$f(gxg^{-1}) \overset{f \text{ hom}}{=} f(g)f(x)f(g^{-1}) \overset{\text{(II)}}{=} f(g)f(x)(f(g))^{-1}.$$

Como $x \in f^{-1}(T)$ tenemos que $f(x) \in T$ y, como $T \lhd H$, por la Proposición I.5.19, $f(g)f(x)(f(g))^{-1} \in T$. En consecuencia, vemos que $gxg^{-1} \in f^{-1}(T)$ y, de nuevo por la Proposición I.5.19, concluimos que $f^{-1}(T) \lhd G$.

■

Observación I.6.5 El análogo de la propiedad (V) para la imagen directa es, en general, falso. En otra palabras, si S es subgrupo normal de G, $f(S)$ no es en general un subgrupo normal de H como muestra el siguiente ejemplo.

Ejemplo I.6.6 Consideramos la inclusión canónica $i :< b_1 > \to D_3$. Como todo grupo es normal en sí mismo, tenemos que $< b_1 > \lhd < b_1 >$ pero $i(< b_1 >) =< b_1 >$ no es normal el D_3, ver Ejemplo I.5.21.

Proposición I.6.7 Sean $(G,\cdot)$, $(H,\cdot)$ y $(K,\cdot)$ tres grupos y $f : G \to H$, $g : H \to K$ dos homomorfismos de grupos. Probar que:

(I) $g \circ f : G \to K$ es un homomorfismo de grupos.

(II) Si f es un isomorfismo, entonces la aplicación inversa $f^{-1} : H \to G$ es un isomorfismo.

Demostración. (I) Dados $a,b \in G$ basta observar que

$$(g \circ f)(ab) = g(f(ab)) \overset{f \text{ hom.}}{=} g(f(a)f(b)) \overset{g \text{ hom.}}{=} g(f(a))g(f(b)).$$

(II) Dados $b_1,b_2 \in H$, como f es isomorfismo f es biyectiva, luego existen $a_1,a_2 \in G$ únicos tales que $f(a_1) = b_1$ y $f(a_2) = b_2$. Por tanto, vemos que

$$f^{-1}(b_1b_2) = f^{-1}(f(a_1)f(a_2)) \overset{f \text{ hom.}}{=} f^{-1}(f(a_1a_2)) \overset{f^{-1} \circ f = \text{Id}}{=} a_1a_2 = f^{-1}(b_1)f^{-1}(b_2).$$

■

Definición I.6.8 Sean $(G,\cdot)$ y $(H,\cdot)$ dos grupos y $f : G \to H$ un homomorfismo de grupos.

(A) llamamos **núcleo de** f a $f^{-1}(\{1_H\})$ y lo denotamos por $\text{Ker}f := f^{-1}(1_H)$.

(B) llamamos **imagen de** f a $f(G)$ y lo denotamos por $\text{Im}f := f(G)$.

Observación I.6.9 Por las Propiedades I.6.4, tenemos que $\text{Im}f$ es un subgrupo de H, porque G es subgrupo de G, y que $\text{Ker}f$ es un subgrupo normal de G, porque $\{1_H\} \lhd H$.

Ejemplos I.6.10 Con la notación de los Ejemplos I.6.3:

(1) Para la aplicación constante tenemos que $\mathrm{Ker} f = G$ y que $\mathrm{Im} f = \{1_H\}$.

(2) Para cada $m \in \mathbb{Z}$, tenemos que $\mathrm{Ker}(f_m) = \{0\}$, $\mathrm{Im}(f_m) = m\mathbb{Z}$, $\mathrm{Ker}(g_m) = m\mathbb{Z}$ y $\mathrm{Im}(g_m) = \mathbb{Z}/m\mathbb{Z}$.

(3) Para la inclusión y la aplicación de paso al cociente, $\mathrm{Ker}(i) = \{1_G\}$, $\mathrm{Im}(i) = G$, $\mathrm{Ker}(p_N) = N$ y $\mathrm{Im}(p_N) = G/N$.

El núcleo nos permite caracterizar la inyectividad.

Proposición I.6.11 Sean $(G,\cdot)$ y $(H,\cdot)$ dos grupos y $f : G \to H$ un homomorfismo de grupos. Se cumple que:

$$f \text{ es inyectivo si y sólo si } \mathrm{Ker} f = \{1_G\}.$$

Demostración. $(\Rightarrow)$ Supongamos que f es inyectivo. Dado $a \in \mathrm{Ker} f$, tenemos que $f(a) = 1_H$ y, por la Propiedad I.6.4.(I), sabemos que $f(1_G) = 1_H$. Por tanto, se tiene que $f(a) = 1_H = f(1_G)$ y, como f es inyectivo, deducimos que $a = 1_G$, luego $\mathrm{Ker} f = \{1_G\}$.

$(\Leftarrow)$ Supongamos que $\mathrm{Ker} f = \{1_G\}$. Dados $a,b \in G$ tales que $f(a) = f(b)$, multiplicando por $(f(b))^{-1}$ a ambos lados vemos que $f(a)(f(b))^{-1} = 1_H$. Por la Propiedad I.6.4.(II), tenemos que $f(a)f(b^{-1}) = 1_H$ y, como f es homomorfismo, $f(ab^{-1}) = 1_H$. Por tanto, $ab^{-1} \in \mathrm{Ker} f = \{1_G\}$, es decir, $ab^{-1} = 1_G$ y, multiplicando por b, concluimos que $a = b$, luego f es inyectivo. ■

Proposición I.6.12 — Orden de un elemento, grupos cíclicos y homomorfismos. Sean $(G,\cdot)$ y $(H,\cdot)$ dos grupos, $a \in G$, $f : G \to H$ un homomorfismo de grupos. Se cumple que:

(I) si $O(a) < \infty$, entonces se tiene que $O(f(a)) < \infty$ y $O(f(a))$ divide a $O(a)$.

(II) si G es cíclico, con $G =< a >$, entonces f está determinado por $f(a)$, es decir, la imagen de todo elemento se puede hallar conociendo la imagen de a de forma única.

(III) si G es cíclico y finito, con $G =< a >$ y $\#G = n$, entonces para cada $b \in H$ tal que $O(b) \mid n$ existe un único homomorfismo $f_b : G \to H$ tal que $f_b(a) = b$.

Demostración. (I) Si $O(a) = r \in \mathbb{N}_{\geq 1}$, entonces $a^r = 1_G$. Observamos que

$$(f(a))^r = f(a)\cdots(\text{r veces})\cdots f(a) \overset{f \text{ hom.}}{=} f(a^r) = f(1_G) \overset{\text{Prop. I.6.4.(I)}}{=} 1_H.$$

Por consiguiente, por la Propiedad I.3.13.(III), $O(f(a)) \mid r$.

(II) Dado $h \in f(G)$, existe $c \in G$ tal que $f(c) = h$. Como $G =< a >$, existe $m \in \mathbb{Z}$ tal que $c = a^m$, luego, como f es homomorfismo, tenemos que $h = f(c) = f(a^m) = (f(a))^m$

(III) Dado $b \in H$ tal que $\ell = O(b) \mid n$, como los elementos de $G =< a >$ son de la forma a^m con $m \in \mathbb{Z}$, definimos $f_b : G \to H$ por $f_b(a^m) := b^m$ para cada $m \in \mathbb{Z}$.
Comprobamos que
□ f_b **está bien definido:** porque si $a^t = a^s$ para $t,s \in \mathbb{Z}$, entonces $n \mid (t-s)$, por la Propiedad I.3.13, luego $\ell \mid (t-s)$ y, de nuevo por la Propiedad I.3.13, tenemos que $b^t = b^s$, es decir, $f_b(a^t) = f_b(a^s)$.
□ f_b **es homomorfismo de grupos:** porque dados $a^t, a^s \in G$ tenemos que

$$f_b(a^t a^s) = f_b(a^{t+s}) = b^{t+s} = b^t b^s = f_b(a^t) f_b(a^s).$$

□ f_b es único por (II).

■

Ejemplos I.6.13 La Proposición I.6.12 nos sirve para determinar todos los posibles homomorfismos que parten de un grupo cíclico y finito $G=<a>$ con llegada en un grupo cualquiera H. Para determinar los posibles homomorfismos basta determinar $\{b\in H\,:\,O(b)\mid O(a)=\#G\}$. Por ejemplo, para determinar todos los posibles homomorfismos $f:(\mathbb{Z}/100\mathbb{Z},+)\to(\mathbb{Z}/120\mathbb{Z},+)$, como $\mathbb{Z}/100\mathbb{Z}=<1>$ y $O(1)=\#(\mathbb{Z}/100\mathbb{Z})=100$ basta determinar todos los elementos de $\mathbb{Z}/120\mathbb{Z}$ cuyo orden divide a 100. Por otro lado, sabemos por el Ejercicio I.3.20 que el orden de un elemento $b\in\mathbb{Z}/120\mathbb{Z}$ cumple que $O(b)\cdot\text{m.c.d.}(120,b)=120$, luego $O(b)\mid 120$. Como $O(b)$ debe dividir a 100 y a 120, tenemos que $O(b)\mid\text{m.c.d.}(100,120)$, es decir, $O(b)\mid 20$. En resumen, se tiene que

$$\{b\in\mathbb{Z}/120\mathbb{Z}\,:\,O(b)\mid 100\}\overset{b\in\mathbb{Z}/120\mathbb{Z}}{=}\{b\in\mathbb{Z}/120\mathbb{Z}\,:\,O(b)\mid 20\}\overset{\text{Prop. I.3.16}}{=}G_{20}=<\frac{120}{20}\cdot 1>=<6>$$

Consecuentemente, hay $\#<6>=20$ posibles homomorfismos de $f:(\mathbb{Z}/100\mathbb{Z},+)\to(\mathbb{Z}/120\mathbb{Z},+)$ uno para cada elemento del único subgrupo de orden 20 de $\mathbb{Z}/120\mathbb{Z}$, es decir, elegimos $f(1)\in\{0,6,12,18,24,20,36,42,48,54,60,66,72,78,84,90,96,102,108,114\}$.

Observación I.6.14 Del mismo modo que se describió en la Notación I.1.4 y I.5.4, dada la relevancia de los homomorfismos resulta conveniente transcribir la definición y algunas de las propiedades que hemos probado.

	Notación multiplicativa $(G,\bullet)\xrightarrow{f}(H,\bullet)$	**Notación aditiva** $(G,+)\xrightarrow{f}(H,+)$
Definición	$f(a\bullet_G b)=f(a)\bullet_H f(b)$	$f(a+_G b)=f(a)+_H f(b)$
Neutro	$f(1_G)=1_H$	$f(0_G)=0_H$
Opuesto	$f(a^{-1})=(f(a))^{-1}$.	$f(-a)=-f(a)$
Núcleo	$f^{-1}(1_H)$	$f^{-1}(0_H)$

¡Ojo! Existen homomorfismos de grupos entre grupos aditivos y multiplicativos. Por ejemplo: $\log:(\mathbb{R}_{>0},\cdot)\to(\mathbb{R},+)$ dada por $f(x)=\log(x)$ es un homomorfismo de grupos. De hecho es un isomorfismo de grupos y su inversa $\exp:(\mathbb{R},+)\to(\mathbb{R}_{>0},\cdot)$ dada por $f(x)=e^x$ es también un homomorfismo de grupos.

I.6.2 Teoremas de isomorfía

Lema I.6.15 — Homomorfismo inducido en el cociente. Sean $(G,\bullet)$ y $(H,\bullet)$ dos grupos, $f:G\to H$ un homomorfismo de grupos y $N\lhd G$ con $N\subseteq\text{Ker}f$. Entonces existe un único homomorfismo $\overline{f}:G/N\to H$ tal que para todo $a\in G$ se tiene que $\overline{f}(aN)=f(a)$.

Demostración. Basta definir $\overline{f}(aN):=f(a)$ para todo $a\in G$ y comprobar que $\overline{f}$ está bien definido y que es homomorfismo de grupos, dado que la unicidad es inmediata porque en la definición estamos diciendo como calcular la imagen de **todo** elemento. Observamos que

- □ $\overline{f}$ **está bien definido:** porque si $aN=bN$ entonces $b^{-1}a\in N\subseteq\text{Ker}f$. Por tanto, $1_H=f(b^{-1}a)=(f(b))^{-1}f(a)$, luego multiplicando por $f(b)$ a ambos lados, $f(a)=f(b)$ y deducimos que $\overline{f}(aN)=f(a)=f(b)=\overline{f}(bN)$.
- □ $\overline{f}$ **es homomorfismo:** porque dados $aN,bN\in G/N$ tenemos que $\overline{f}(aNbN)=\overline{f}((ab)N)=f(ab)\overset{f\text{ hom.}}{=}f(a)f(b)=\overline{f}(aN)\overline{f}(bN)$.

■

Ejemplo I.6.16 Para el homomorfismo $f:(\mathbb{Z},+)\to(\mathbb{Z}/12\mathbb{Z},+)$ dado por $f(a)=3a+12\mathbb{Z}$ se tiene que $\mathrm{Ker}f=4\mathbb{Z}$, luego eligiendo $N=24\mathbb{Z}\subseteq 4\mathbb{Z}$, por el Lema, existe un único homomorfismo $\overline{f}:(\mathbb{Z}/24\mathbb{Z},+)\to(\mathbb{Z}/12\mathbb{Z},+)$ tal que $\overline{f}(a+24\mathbb{Z})=3a+12\mathbb{Z}$.

Teorema I.6.17 (Primer Teorema de Isomorfía). Sean $(G,\bullet)$ y $(H,\bullet)$ dos grupos y un homomorfismo de grupos $f:G\to H$. Entonces:

$$G\Big/\mathrm{Ker}f\approx \mathrm{Im}f.$$

Demostración. Por el Lema I.6.15 para $N=\mathrm{Ker}f$ existe $\overline{f}:G/\mathrm{Ker}f\to H$ un homomorfismo dado por $\overline{f}(a\mathrm{Ker}f):=f(a)$ para todo $a\in G$. Por definición, se cumple que el subgrupo de llegada es $\mathrm{Im}\overline{f}$ y que $\overline{f}:G/\mathrm{Ker}f\to\mathrm{Im}\overline{f}$ es sobreyectivo. Para concluir basta probar que $\overline{f}$ es inyectivo y que $\mathrm{Im}f=\mathrm{Im}\overline{f}$, de esta forma $\overline{f}:G/\mathrm{Ker}f\to\mathrm{Im}f$ es el isomorfismo buscado.

□ $\overline{f}$ **es inyectivo** porque $\overline{f}(a\mathrm{Ker}f)=1_H$ si y solo si $f(a)=1_H$. Por tanto, si $a\mathrm{Ker}f\in\mathrm{Ker}\overline{f}$, entonces $a\in\mathrm{Ker}f$ y se cumple que $a\mathrm{Ker}f=1_G\mathrm{Ker}f=1_{G/\mathrm{Ker}f}$, luego $\mathrm{Ker}\overline{f}=\{1_{G/\mathrm{Ker}f}\}$ y concluimos que $\overline{f}$ es inyectivo.

□ $\mathrm{Im}f=\mathrm{Im}\overline{f}$ porque

$$h\in\mathrm{Im}f\ \Leftrightarrow\ \exists\, a\in G \text{ tal que } f(a)=h\ \Leftrightarrow\ \exists\, aN\in G/N \text{ tal que } \overline{f}(aN)=h\ \Leftrightarrow\ h\in\mathrm{Im}\overline{f}.$$

■

Ejemplos I.6.18 (1) Consideramos $f:(\mathbb{R},+)\to(\mathbb{C}\backslash\{0\},\cdot)$ dada por $f(x)=e^{2\pi xi}$ para cada $x\in\mathbb{R}$. Comprobamos que $\mathrm{Ker}f=\mathbb{Z}$ y que $\mathrm{Im}f=S^1=\{z\in\mathbb{C}\,:\,|z|=1\}$, luego por el Primer Teorema de Isomorfía tenemos que $(\mathbb{R}/\mathbb{Z},+)\approx(S^1,\cdot)$.

(2) Consideramos $f:(\mathrm{GL}(n,\mathbb{R}),\cdot)\to(\mathbb{R}\backslash\{0\},\cdot)$ dada por $f(A)=\det(A)$ para cada $A\in\mathrm{GL}(n,\mathbb{R})$. Comprobamos que $\mathrm{Ker}f=\mathrm{SL}(n,\mathbb{R})$ y que f es sobreyectivo, luego por el Primer Teorema de Isomorfía concluimos que

$$\mathrm{GL}(n,\mathbb{R})\Big/\mathrm{SL}(n,\mathbb{R})\approx\mathbb{R}\backslash\{0\}.$$

Corolario I.6.19 (Unicidad de los grupos cíclicos)
(I) Todo grupo cíclico infinito es isomorfo a $(\mathbb{Z},+)$.
(II) Todo grupo cíclico de orden $n\in\mathbb{N}_{\geq 1}$ es isomorfo a $(\mathbb{Z}/n\mathbb{Z},+)$.

Demostración. Dado un grupo cíclico $G=<a>$, consideramos la aplicación f dada por

$$\begin{array}{rccc} f:(\mathbb{Z},+) & \to & (G,\cdot) \\ m & \to & a^m \end{array}$$

Comprobamos que f es un homomorfismo sobreyectivo. Distinguimos dos casos:

(I) Si $\#G=\infty$, entonces $O(a)=\infty$ y dado $m\in\mathbb{Z}$ se cumple que

$$f(m)=1_G\ \Leftrightarrow\ a^m=1_G\ \overset{O(a)=\infty}{\Leftrightarrow}\ m=0\ \Leftrightarrow\ \mathrm{Ker}f=\{0\}.$$

En consecuencia, por el Primer Teorema de Isomorfía $\mathbb{Z}/\{0\}\approx\mathrm{Im}f=G$. Observamos que $\mathbb{Z}/\{0\}\approx\mathbb{Z}$, luego G es isomorfo a $(\mathbb{Z},+)$.

(II) Si $\#G = n$, entonces $O(a) = n$ y dado $m \in \mathbb{Z}$ se cumple que

$$f(m) = 1_G \;\Leftrightarrow\; a^m = 1_G \overset{\text{Prop. I.3.13}}{\Leftrightarrow} n \mid m \;\Leftrightarrow\; m \in n\mathbb{Z}.$$

En consecuencia, $\mathrm{Ker} f = n\mathbb{Z}$ y, por el Primer Teorema de Isomorfía $\mathbb{Z}/n\mathbb{Z} \approx \mathrm{Im} f = G$. ■

Notación I.6.20 Como consecuencia de este corolario podemos decir que los grupos cíclicos son únicos (salvo isomorfismo) y, sin pérdida de generalidad, como todos los grupos cíclicos de orden n son isomorfos denotaremos por C_n a cualquiera de ellos.

Teorema I.6.21 (Segundo Teorema de Isomorfía). Sea $(G,\cdot)$ un grupo, S un subgrupo de G y $N \lhd G$. Entonces

$$S\Big/(N \cap S) \approx (NS)\Big/N.$$

Demostración. Por el Teorema I.5.27, sabemos que $N \cap S \lhd S$, que $NS = SN$ es subgrupo y $N \lhd NS$. Consideramos los homomorfismos:

$$\begin{array}{rcl} i : S & \to & NS \\ s & \to & 1_G \cdot s \end{array} \quad \text{(inyección canónica)} \qquad \begin{array}{rcl} p : NS & \to & NS/N \\ t & \to & tN \end{array} \quad \text{(paso al cociente)}$$

Definimos $f = p \circ i : S \to NS/N$. Sabemos que f es homomorfismo por ser composición de homomorfismos y que es sobreyectivo porque dado $tN \in NS/N$ como $t \in NS = SN$ se tiene que $t = sn$ con $s \in S$ y $n \in N$, luego $s^{-1}t \in N$ y $tN = sN$ y concluimos que $f(s) = p(s) = sN = tN$. Por otro lado, observamos que

$$\mathrm{Ker} f = \{s \in S : f(s) = 1_{NS/N}\} = \{s \in S : sN = 1_G N\} = \{s \in S : s \in N\} = S \cap N.$$

En conclusión, por el Primer Teorema de Isomorfía, $S\Big/(N \cap S) \approx (NS)\Big/N$. ■

Ejemplo I.6.22 En $(\mathbb{Z},+)$ consideramos los subgrupos $N = 3\mathbb{Z}$ y $S = 2\mathbb{Z}$, ambos son normales porque $\mathbb{Z}$ es abeliano. Por tanto, por el Segundo Teorema de Isomorfía, se obtiene que

$$2\mathbb{Z}/(2\mathbb{Z} \cap 3\mathbb{Z}) \approx (2\mathbb{Z} + 3\mathbb{Z})/3\mathbb{Z}.$$

Teorema I.6.23 (Tercer Teorema de Isomorfía). Sean $(G,\cdot)$ un grupo, $N \lhd G$ y $M \lhd G$ tales que $N \subseteq M$. Entonces se cumple que $M/N \lhd G/N$ y que

$$(G/N)\Big/(M/N) \approx (G/M).$$

Demostración. Consideramos $p_M : G \to G/M$ la aplicación de paso al cociente definida por $p_M(a) = aM$ para cada $a \in G$. Observamos que $\mathrm{Ker}(p_M) = M \supseteq N$, luego por el Lema I.6.15 sabemos que existe un único homomorfismo $f = \overline{p_N} : G/N \to G/M$ dado por

$$\begin{array}{rcl} f : \; G/N & \to & G/M \\ aN & \to & aM \end{array}$$

Por el el Lema I.6.15, f está bien definida y es homomorfismo. Comprobamos que f **es sobreyectivo** porque dado $aM \in G/M$ se tiene que $f(aN) = aM$. Por otro lado, observamos que

$$\mathrm{Ker} f = \{aN \in G/N \,:\, f(aN) = 1_{G/M}\} = \{aN \in G/N \,:\, aM = M\} = \{aN \in G/N \,:\, a \in M\} = M/N.$$

En consecuencia, M/N es normal en G/N por ser el núcleo de un homomorfismo y, por el Primer Teorema de Isomofía, se cumple que $(G/N)\Big/(M/N) \approx (G/M)$. ■

Ejemplo I.6.24 En $(\mathbb{Z},+)$ consideramos los subgrupos $N=12\mathbb{Z}$ y $M=3\mathbb{Z}$, que son normales y $12\mathbb{Z}\subseteq 3\mathbb{Z}$. Por el Tercer Teorema de Isomorfía, se tiene que

$$(\mathbb{Z}/12\mathbb{Z})\Big/(3\mathbb{Z}/12\mathbb{Z})\approx(\mathbb{Z}/3\mathbb{Z}).$$

I.6.3 Clasificación de grupos de orden p y $2p$. Grupos de orden pequeño

En esta sección vamos a determinar todos los grupos posibles, no isomorfos, de orden p con p primo y orden $2p$ con p primo y $p>2$. Como consecuencia de esto tenemos una clasificación completa de los grupos de órdenes 2, 3, 5, 6, 7, 10, 11, 13, 14. Con el Ejercicio I.6.45 podemos clasificar los grupos de orden p^2, en particular, los de orden 4 y 9. El ejercicio I.6.58 nos permite clasificar los grupos de orden pq con p y q primos $p<q$ y $p\nmid(q-1)$, en concreto, es válido para orden 15. Finalmente, dado que al aumentar el número de divisores aumenta la cantidad de grupos no isomorfos, los grupos de orden 8, ver Ejercicio I.6.48, y de orden 12, ver Ejercicio I.6.49, se tratan de manera individual.

De esta forma, se obtiene una clasificación completa de los **grupos de orden pequeño** ($\#G<16$). Conviene destacar que la nomenclatura grupo de orden pequeño para $\#G<16$ no es estándar y su naturaleza es puramente práctica dado que la cantidad de grupos no isomorfos de ordenes 1 hasta 15 es 28, 20 abelianos y 8 no abelianos, y para orden exactamente 16 se puede probar que existen 14 grupos no isomorfos, 5 abelianos y 9 no abelianos (¡La mitad de los que teníamos hasta 15!). En otras palabras, aunque hasta orden 15 la clasificación es suficientemente ilustrativa, si se desea se puede continuar con la clasificación de los grupos. En el sistema de álgebra computacional GAP (acrónimo de Groups, Algorithms and Programming) se puede encontrar una base de datos, denominada *'Small Groups library'* que contiene la clasificación completa de los grupos hasta orden 2000, excepto para orden 1024 y, adicionalmente, contiene la clasificación de algunos grupos particulares de orden mayor que 2000 en total más de 400 millones grupos. [*]

Teorema I.6.25 (Grupos de orden p). Sea $(G,\bullet)$ un grupo de orden p con p primo. Entonces se cumple que :

$$G\approx C_p$$

Demostración. Directo del Corolario I.5.14 y del Corolario I.6.19. ■

Proposición I.6.26 Sea G un grupo generado por dos elementos $G=<x,y>$ tal que
(1) $O(x)=n\in\mathbb{N}_{\geq 3}$.
(2) $O(y)=2$.
(3) $yx=x^{-1}y$.
Entonces se cumple que $G\approx D_n$.

Demostración. Por definición tenemos que

$$G=<x,y>=\left\{c_1^{e_1}c_2^{e_2}\cdots c_k^{e_k}\,:\,k\in\mathbb{N}_{\geq 1},\,c_i\in\{x,y\},\,e_i\in\mathbb{Z}\right\}.$$

Por inducción probamos que $\boxed{yx^r=x^{n-r}y \text{ para todo } r\in\mathbb{N}_{\geq 1}}$.
Para $r=1$, por (1), sabemos que $x^n=1_G$ y, por (3), vemos que $yx=x^{-1}y=x^nx^{-1}y=x^{n-1}y$.
Supongamos que se cumple para un cierto $r\in\mathbb{N}_{\geq 1}$. Tenemos que

$$yx^{r+1}\overset{\text{(G.I)}}{=}(yx^r)x\overset{\text{H.I.}}{=}(x^{n-r}y)x\overset{\text{(G.I)}}{=}x^{n-r}(yx)\overset{(3)}{=}x^{n-r}x^{-1}y=x^{n-(r+1)}y.$$

[*] https://www.gap-system.org/Packages/smallgrp.html

Por consiguiente, por el Principio de Inducción queda demostrada la propiedad.
En consecuencia, razonando de nuevo por inducción, dada una expresión de la forma $c_1^{e_1}c_2^{e_2}\cdots c_k^{e_k}$ con $k\in\mathbb{N}_{\geq 1}$, $c_i\in\{x,y\}$ y $e_i\in\mathbb{Z}$ se puede transformar en una expresión de la forma x^jy^i con $i,j\in\mathbb{Z}$ usando la propiedad que acabamos de probar. Por (1) y (2), realizando la división euclídea de los exponentes entre n y 2 respectivamente, podemos además concluir que los elementos de G son de la forma x^jy^i con $j\in\{0,1,\ldots,n-1\}$ y $i\in\{0,1\}$. En consecuencia, se tiene que

$$G=\{x^jy^i : j\in\{0,1,\ldots,n-1\} \text{ y } i\in\{0,1\}\}.$$

Observamos que los elementos son dos a dos distintos, es decir, si $x^jy^i=x^sy^t$ con $j,s\in\{0,1,\ldots,n-1\}$ y $i,t\in\{0,1\}$ porque

(a) Si $i=t=0$, entonces $x^j=x^s$ y como $O(x)=n$ y $j,s\in\{0,1,\ldots,n-1\}$, concluimos que $j=s$.
(b) Si $i=t=1$, entonces $x^jy=x^sy$. Como $O(y)=2$, multiplicando por y a ambos lados, vemos que $x^j=x^jy^2=x^sy^2=x^s$ y como en (a), concluimos que $j=s$.
(c) Si $i=1$ y $t=0$ (o viceversa) entonces $x^jy=x^s$, luego $y=x^{s-j}\in<x>$. En este caso tendríamos que $y=x^\ell$ conmuta con x, es decir, $xy=yx\overset{(1)}{=}x^{-1}y$ y, multiplicando por y, deduciríamos que $x=x^{-1}$ luego $O(x)=2$ (Imposible).

Finalmente, con la notación del Ejercicio I.4.35, comprobamos de forma directa que

$$\begin{array}{rccc} f: & D_n & \to & G \\ & r^is^j & \to & x^iy^j \end{array}$$

es un isomorfismo. ■

Ejemplos I.6.27 (1) Comprobamos que el subgrupo $S=<x=(12\,456),y=(26)(45)>$ de S_6 es isomorfo a D_5 usando la proposición anterior.
(2) Fijado $n\in\mathbb{N}_{\geq 1}$, $n\geq 3$, Comprobamos que el subgrupo

$$S=<X=\begin{pmatrix}\cos(2\pi/n) & -\operatorname{sen}(2\pi/n)\\ \operatorname{sen}(2\pi/n) & \cos(2\pi/n)\end{pmatrix},\ Y=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}>$$

de $GL(n,\mathbb{C})$ es isomorfo a D_n usando la proposición anterior.

Teorema I.6.28 (Grupos de orden $2p$). Sea $(G,\bullet)$ un grupo de orden $2p$ con p primo y $p>2$. Entonces se cumple que:

O bien G es isomorfo a D_p o bien G es isomorfo a C_{2p}

Demostración. En primer lugar, observamos que D_p y C_{2p} no son isomorfos porque D_p no es cíclico. Distinguimos dos casos:

(a) G **posee algún elemento** $a\in G$ **de orden** $2p$, entonces $O(a)=\#<a>=2p$. Como $\#G=2p$, deducimos que $G=<a>$ y concluimos que $G\approx C_{2p}$ por el Corolario I.6.19.
(b) G **no posee elementos de orden** $2p$, entonces por el Corolario I.5.13 para cada $a\in G$ distinto de 1_G se tiene que o bien $O(a)=2$ o bien $O(a)=p$.

Razonamos por reducción al absurdo y suponemos que todos los elementos de G tienen orden 2. Como $\#G=2p>4$ porque $p>2$, existen $a,b\in G$ con $a\neq b$, $a\neq 1_G$ y $b\neq 1_G$. Observamos que

$$ab\overset{O(a)=O(b)=2}{=}b^2aba^2\overset{\text{(G.I)}}{=}b(ba)(ba)a\overset{O(ba)=2}{=}ba.$$

Por consiguiente, $S=\{1,a,b,ab\}$ sería un subgrupo de G de orden 4 y, por el Teorema de Lagrange, tendríamos que $4\mid 2p$ (Imposible porque p es primo con $p>2$).

Por tanto, existe algún elemento $a \in G$ con $O(a) = p$.
Como $\#G = 2p$ y $\# < a >= O(a) = p$, existe $b \in G$ con $b \notin < a >$. Veamos que $O(b) = 2$. Razonamos por reducción al absurdo y suponemos que $O(b) = p$. Como, por el Teorema de Lagrange, $\#(< a > \cap < b >)$ divide a $\# < b >= p$, y como se cumple que $< b > \not\subseteq < a >$, deducimos que $< a > \cap < b > \subsetneq < b >$ y que $\#(< a > \cap < b >) = 1$. Por el Lema I.5.26, se tiene que

$$\#(< a >< b >) = \frac{\# < a > \# < b >}{\#(< a > \cap < b >)} = p^2.$$

Esto es imposible porque $p^2 > 2p = \#G$ y $< a >< b > \subseteq G$.
En resumen, tenemos $a \in G$ con $O(a) = p$ y $b \notin < a >$ con $O(b) = 2$. Observamos que $a^{-1}b \notin < a >$ porque $b \notin < a >$, luego de la misma forma se preuba que $O(a^{-1}b) = 2$. En consecuencia, vemos que

$$ba \overset{O(b)=2}{=} b^{-1}(a^{-1})^{-1} = (a^{-1}b)^{-1} \overset{O(a^{-1}b)=2}{=} a^{-1}b.$$

Por la Proposición I.6.26, se tiene que $< a,b >\approx D_p$ y, como $< a,b > \subseteq G$ y $\# < a,b >= 2p = \#G$, concluimos que $G =< a,b >\approx D_p$.

■

La información de este bloque se ha elaborado empleando principalmente el libro [8] que se recomienda consultar para completar la información.

Ejercicio I.6.29 Comprobar que las siguientes aplicaciones son homomorfismos. Determinar su núcleo y su imagen.

(I) $f : (\mathrm{GL}(n,\mathbb{R}),\cdot) \to (\mathbb{R}\backslash\{0\},\cdot)$ dada por $f(A) = \det(A)$.
(II) $f : (\mathrm{GL}(n,\mathbb{R}),\cdot) \to (\mathbb{R}_{>0},\cdot)$ definida por $f(A) = |\det(A)|$.
(III) $f : (\mathbb{C}\backslash\{0\},\cdot) \to (\mathbb{R}\backslash\{0\},\cdot)$ dada por $f(a+bi) = a^2+b^2$.
(IV) $f : (\mathbb{Z}\oplus\mathbb{Z},+) \to (\mathbb{Z},+)$ tal que $f(a,b) = a$.
(V) $f : (\mathbb{R}\backslash\{0\},\cdot) \to (\mathbb{R}\backslash\{0\},\cdot)$ dada por $f(a) = |a|$.
(VI) $f : (\mathbb{Z}\oplus\mathbb{Z},+) \to (\mathbb{Z},+)$ tal que $f(a,b) = a+3b$.
(ver Ejercicios I.1.9 para la definición de $\mathbb{Z}\oplus\mathbb{Z}$)

Ejercicio I.6.30 Sea G un grupo y $N \lhd G$. Demostrar que cada subgrupo de G/N es de la forma K/N para algún subgrupo K de G que contiene a N. Determinar todos los subgrupos de $D_4/\langle a^2\rangle$ (Sugerencia: emplear Ejercicio I.6.32).

Ejercicio I.6.31 Describir todos los homomorfismos existentes $f : G \to H$ para los siguientes pares de grupos G,H

(I) $G = \mathbb{Z}/100\mathbb{Z}$ y $H = \mathbb{Z}/30\mathbb{Z}$.

(II) $G = \mathbb{Z}/30\mathbb{Z}$ y $H = \mathbb{Z}/100\mathbb{Z}$.

(III) $G = \mathbb{Z}/n\mathbb{Z}$ y $H = \mathbb{Z}$.

(IV) $G = \mathbb{Z}/40\mathbb{Z}$ y $H = \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}$.

(V) $G = H = \mathbb{Z}$.

(VI) $G = \mathbb{Z}$ y $H = \mathbb{Q}$.

Ejercicio I.6.32 Dado un homomorfismo de grupos $f : G \to H$ sobreyectivo, probar que existe una biyección entre los subconjuntos:

$$\mathscr{S} = \{S : S \text{ es subgrupo de } G \text{ y } \mathrm{Ker} f \subseteq S\}, \qquad \mathscr{T} = \{T : T \text{ es subgrupo de } H\},$$

de modo que se hace corresponder subgrupos normales con subgrupos normales.

Ejercicio I.6.33 Determinar todos los automorfismos $f : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$.

Ejercicio I.6.34 Sean $(G,\bullet)$ y $(H,\bullet)$ dos grupos cíclicos y finitos con $\#G = n$ y con $\#H = m$. Probar que si $d = \text{m.c.d.}(n,m)$ entonces hay d homomorfismos distintos de G en H. Mostrar con un ejemplo que esto no es cierto si H no es cíclico.

Ejercicio I.6.35 Aplicar el Primer Teorema de Isomorfía a cada uno de los homomorfismos dados en el Ejercicio I.6.29. Para los homomorfismos (IV) y (VI) del Ejercicio I.6.29, se considera el subgrupo $N = \langle (10,1) \rangle$ de $\mathbb{Z} \oplus \mathbb{Z}$. Elegir un subgrupo M de $\mathbb{Z}$ de forma que la aplicación dada por

$$N \to f(a,b) + M,$$

sea homomorfismo. Calcular en cada uno de los casos, el núcleo y la imagen de dicho homomorfismo.

Ejercicio I.6.36 Sea $f : G \to H$ un homomorfismo de grupos y S un subgrupo de G. Probar que:
(I) Si S es cíclico, entonces $f(S)$ es cíclico.
(II) Si S es abeliano, entonces $f(S)$ es abeliano,
(III) Si $\#(\mathrm{Ker} f) = m$, entonces para cada $h \in f(G)$ se tiene que $\#f^{-1}(h) = m$.
(IV) Si $\#S < \infty$, entonces $\#f(S)$ divide a $\#S$.
Mostrar con un ejemplo en cada caso que el recíproco es falso.

Ejercicio I.6.37 Dados G y H dos grupos isomorfos. Probar que:
(I) G es cíclico si y solo si H es cíclico.
(II) G es abeliano si y solo si H es abeliano.
(III) G tiene $m \in \mathbb{N}$ elementos de orden n si y solo si H tiene $m \in \mathbb{N}$ elementos de orden n.
(IV) G tiene $k \in \mathbb{N}$ subgrupos de orden d si y solo si H tiene $k \in \mathbb{N}$ subgrupos de orden d.

Ejercicio I.6.38 Probar que $(\mathbb{Q},+) \not\approx (\mathbb{Q}\backslash\{0\},\cdot)$.

Ejercicio I.6.39 Probar que $(\mathbb{Z} \oplus \mathbb{Z})/\langle \{(n,0),\ (0,m)\} \rangle$ es isomorfo a $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.

Ejercicio I.6.40 Sean G un grupo abeliano y H y K subgrupos de G. Probar que las siguientes afirmaciones son falsas en general:
(I) Si $H \approx K$, entonces $G/H \approx G/K$.
(II) Si $H \not\approx K$, entonces $G/H \not\approx G/K$
(Pista: Considerar el grupo producto $(\mathbb{Z}/4\mathbb{Z},+) \times (U(\mathbb{Z}/4\mathbb{Z}),\cdot)$ en ambos apartados)
(Repista: en el primer apartado considerar $H = \langle (2,3) \rangle$ y $K = \langle (2,1) \rangle$)

Ejercicio I.6.41 Sea G el grupo $(U(\mathbb{Z}/16\mathbb{Z}),\cdot)$, $H = \langle 15 \rangle$ y $K = \langle 9 \rangle$. ¿Es $H \approx K$?¿Es $G/H \approx G/K$?

Ejercicio I.6.42 Dado $f: G \to H$ un homomorfismo de grupos $N \lhd G$ y $M \lhd H$ con $f(N) \subseteq M$. Probar que f induce un homomorfismo $\overline{f}: G/N \to H/M$ dado por $\overline{f}(aN) = f(a)M$ para cada $aN \in G/N$. ¿Es $\overline{f}$ único?

Ejercicio I.6.43 (Teorema de Cayley). Dado $(G,\cdot)$ un grupo, $a \in G$ definimos la aplicación multiplicación a la izquierda por a por

$$\begin{array}{rccc} T_a: & G & \to & G \\ & b & \to & ab \end{array}$$

Probar que:

(I) T_a es biyectiva y deducir que T_a es una permutación de G, es decir, $T_a \in S(G)$.

(II) $\mathcal{T} = \{T_a : a \in G\}$ es un subgrupo de $(S(G), \circ)$.

(III) $f: G \to \mathcal{T}$ dado por $f(a) = T_a$ es un isomorfismo de grupos.

(IV) **[Teorema de Cayley]** Todo grupo $(G,\cdot)$ es isomorfo a un subgrupo de permutaciones de $(S(G),\circ)$. En particular, si G es un grupo de orden $n \in \mathbb{N}_{\geq 1}$, G es isomorfo a un subgrupo de S_n.

Ejercicio I.6.44 Encontrar un subgrupo de S_n isomorfo a $(U(\mathbb{Z}/12\mathbb{Z}),\cdot)$ con $n = \#U(\mathbb{Z}/12\mathbb{Z})$.

Ejercicio I.6.45 (Grupos de orden p^2). Sea G un grupo finito con $\#G = p^2$, con p primo. Probar que G es conmutativo. El objetivo de este ejercicio es demostrar que

o bien G es isomorfo a C_{p^2} o bien es isomorfo a $C_p \times C_p$.

(I) Si G tiene un elemento de orden p^2, deducir que es isomorfo a C_{p^2}.

(II) Si ninguno de los elementos G tiene orden p^2, se pide:

(II.a) Probar que todo elemento de G, distinto del neutro, tiene orden p.

(II.b) Fijados dos elementos $x, y \in G$, distintos del neutro y con $x \notin < y >$, probar que $< x > \cap < y > = \{1_G\}$.

(II.c) Probar que el conjunto $\{x^i y^j : i, j \in \{0,1,\ldots,p-1\}\}$ tiene p^2 elementos distintos y deducir que es igual a G.

(II.d) Si $H = < y >$, probar que $Hx \subseteq \cup_{i=1}^{p-1} Hx^i$ y deducir que tiene que haber dos elementos de Hx en $x^i H$ para algún $i \in \{1,2,\ldots,p-1\}$.

(II.e) Empleando los dos elementos del resultado anterior, probar que existen $m, n \not\equiv 0$ mód p tales que $xy^m x^{-1} = y^n$.

(II.f) Deducir que $xyx^{-1} = y^N$ y, razonando por inducción, que $x^r y x^{-r} = y^{N^r}$ y concluir que $xyx^{-1} = y$.

(II.g) Deducir que x e y conmutan y probar que G es abeliano.

(II.h) Probar que la aplicación $\Phi: \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G$ dada por $\Phi(i,j) = x^i y^j$ es un isomorfismo de grupos.

Ejercicio I.6.46 Dados $n, m \in \mathbb{N}_{\geq 1}$. Probar que

$$\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} \approx \mathbb{Z}/(nm)\mathbb{Z} \qquad \Leftrightarrow \qquad \text{m.c.d.}(n,m) = 1.$$

Obsérvese que se puede reescribir como $C_n \times C_m \approx C_{nm}$ de acuerdo con la Notación I.6.20.

Ejercicio I.6.47 Probar que si m,n son dos enteros positivos primos entre sí, la aplicación

$$\begin{aligned} f : (U(\mathbb{Z}/(mn)\mathbb{Z}),\cdot) &\to (U(\mathbb{Z}/m\mathbb{Z}),\cdot)\times(U(\mathbb{Z}/n\mathbb{Z}),\cdot) \\ x+(mn)\mathbb{Z} &\to \quad (\ x+m\mathbb{Z},\quad x+n\mathbb{Z}\ ). \end{aligned}$$

es isomorfismo de grupos. Deducir que $\varphi(mn)=\varphi(n)\varphi(m)$ (ver Ejercicio A.2.28).

Ejercicio I.6.48 (Grupos de orden 8). Sea G un grupo de orden 8. Probar que:

(I) Si G es abeliano, entonces G es isomorfo a alguno de los tres siguientes grupos:

$$\text{o bien} \quad C_8 \quad \text{o bien} \quad C_2\times C_4 \quad \text{o bien} \quad C_2\times C_2\times C_2.$$

(II) Si G no es conmutativo, entonces G es isomorfo a alguno de los dos siguientes grupos:

$$\text{o bien} \quad D_4 \quad \text{o bien} \quad Q_8.$$

Ejercicio I.6.49 (Grupos de orden 12). Dar el ejemplo de cinco grupos de orden 12 no isomorfos entre sí, razonando porque no son isomorfos.

Ejercicio I.6.50 (Descomposición de grupos abelianos). Sea G un grupo abeliano de orden $\#(G)=a\cdot b$ con m.c.d.$(a,b)=1$. El objetivo de este ejercicios es probar que G existen dos subgrupos A y B de G con $\#(A)=a$ y $\#(B)=b$ de forma que G es isomorfo al grupo producto, ver Ejercicio I.1.9 de A por B, es decir, $A\times B\simeq G$. Para ello se pide:

(I) Probar que para cada $m\in\mathbb{N}_{\geq 1}$ se tiene que $S_m=\{x\in G\,:\,x^m=1_G\}$ es un subgrupo de G.

(II) Llamamos $A=S_a$ y $B=S_b$. Probar que $G=AB$.
(Pista: Hacer uso de la Identidad de Bezout)

(III) Probar que $A\cap B=\{1_G\}$.

(IV) Probar que la aplicación $f:A\times B\to G$ dada por $f(x,y)=xy$ es un isomorfismo.

(V) Probar que $\#A=a$ y $\#B=b$. *(Pista emplear el Lema I.5.26 y el Teorema de Cauchy)*

Ejercicio I.6.51 (Grupos abelianos de orden p^n). Sea G un grupo abeliano de orden p^n con p primo. El objetivo del ejercicios es probar que G es un producto directo de grupos cíclicos.
Sea $a\in G$ un elemento de orden máximo en G, es decir, $O(a)=p^m$ y para todo $g\in G$ se tiene que $O(g)\leq p^m$.

(I) Si $G\neq<a>$ y tomamos b del menor orden posible tal que $b\notin<a>$, probar que $O(b)=p$ y deducir que $<a>\cap<b>=\{1_G\}$.

(II) Si $N=<b>$ tomando b como en el apartado anterior, probar que $O(aN)=O(a)=p^m$.

(III) Probar, por inducción en $\#G$, que $G\simeq<a>\times K$ con a el elemento de orden máximo y K un subgrupo (eventualmente trivial) de G.
(Pista: En el paso inductivo considerar el cociente G/N probar que descompone como $<aN>\times\tilde{K}$ y deducir que $G=<a>K$ con $K=p_N^{-1}(\tilde{K})$)

(IV) Probar, por inducción haciendo uso del apartado anterior, que

$$G\approx C_{p^{m_1}}\times C_{p^{m_2}}\times\ldots\times C_{p^{m_r}}$$

Ejercicio I.6.52 (Teorema fundamental de grupos abelianos finitos (Kronecker, 1858)). Probar que todo grupo abeliano finito G es isomorfo a un producto directo de grupos cíclicos de orden de una potencia de un número primo. Además, el número de términos en el producto y los órdenes de los grupos cíclicos están determinados únicamente por el grupo. En otras palabras

$$G \approx C_{p_1^{k_1}} \times C_{p_2^{k_2}} \times \ldots \times C_{p_r^{k_r}},$$

donde $p_1, p_2, \ldots, p_r$ son números primos y $k_1, k_2 \ldots, k_r \in \mathbb{N}_{\geq 1}$ y los enteros $p_1^{k_1}, p_2^{k_2}, \ldots, p_r^{k_r}$ (no necesariamente distintos) son únicos salvo por el orden. (Para más información consultar [8, Capítulo 11]).

Descomponemos la prueba en los siguientes pasos:

(I) Probar que todo grupo abeliano finito, no trivial, es isomorfo a un producto directo de grupos abelianos finitos de orden la potencia de un primo. En concreto, si $\#G = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s}$ con q_i primos positivos distintos dos a dos, entonces $G \simeq H_1 \times \cdots \times H_s$ con H_i subgrupo de G con $\#(H_i) = q_i^{\alpha_i}$
(Pista: Razonar por inducción en el orden de G empleando el Ejercicio I.6.50)

(II) Aplicar el Ejercicio I.6.51 para probar que para todo $i \in \{1, \ldots, s\}$ se tiene que H_i es un producto directo de grupos cíclicos y deducir la descomposición deseada para G.

Ejercicio I.6.53 (Clases de Conjugación). Sean $a, b \in G$, decimos que a y b son conjugados en G, si existe $x \in G$ tal que $xax^{-1} = b$. La **clase de conjugación de** a es el conjunto

$$c\ell(a) := \{xax^{-1} : x \in G\}.$$

(I) Probar que aRb si y sólo si $b \in c\ell(a)$ define una relación de equivalencia.
(II) Deducir que $[a]_R = c\ell(a)$.
(III) Probar que $c\ell(a) = \{a\}$ si y solamente si $a \in Z(G)$.
(IV) Calcular las clases de conjugación en Q_8 (ver Ejercicio I.2.22).

Ejercicio I.6.54 (Centralizador de un elemento). Dado un grupo $(G, \cdot)$ y un elemento $g \in G$ definimos.

$$C(g) = \{a \in G : ag = ga\}.$$

Probar que:

(I) $C(g)$ es un subgrupo de G.
(II) $Z(G) = \cap_{g \in G} C(g)$. (Ver Ejercicio I.2.21)
(III) $C(g) = C(g^{-1})$ y para todo $k \in \mathbb{Z}$, $C(g) \subseteq C(g^k)$
(IV) $\langle g \rangle$ es un subgrupo de $C(g)$.

Ejercicio I.6.55 (Número de clases de conjugación). Sea G un grupo finito y $a \in G$. Consideramos la aplicación ψ_a definida como

$$\begin{array}{rccc} \psi_a : & G & \to & c\ell(a) \\ & x & \to & xax^{-1} \end{array}$$

Probar que:

(I) para todo $b \in c\ell(a)$, con $yay^{-1} = b$, se tiene que $\psi_a^{-1}(b) = y\,C(a)$
(ver E. I.6.54 y E. I.6.53 para la notación).
(II) para todo $x \in G$ se tiene que $\#(xC(a)) = \#C(a)$.

(III) $\#G = \sum_{b \in c\ell(a)} \#\psi_a^{-1}(b)$ y concluir que $\#G = \#c\ell(a)\#C(a)$.

Ejercicio I.6.56 ($p-$Grupos). Un grupo finito G se dice que es un $p-$**grupo** cuando existe p primo y $k \in \mathbb{N}_{\geq 1}$ tal que $\#G = p^k$. Denotamos por $G/R = \{c\ell(x); x \in G\}$ el conjunto de clases de equivalencia definidas por la relación R en el Ejercicio I.6.53. Empleando los Ejercicios I.6.53 y I.6.55, si G es un $p-$grupo, se pide

(I) Probar que:

$$\#G = \sum_{c\ell(x) \in G/R} \#c\ell(x) = \#Z(G) + \sum_{c\ell(x) \in G/R \atop \#c\ell(x) > 1} \#c\ell(x).$$

(II) Probar que para todo $a \in G \backslash Z(G)$ se tiene que $\#c\ell(a) \geq 2$ y deducir que existe $\ell \in \mathbb{N}_{\geq 1}$ tal que $p^\ell \mid \#c\ell(a)$. Concluir que $p \mid \#Z(G)$.

(III) Probar que **el centro de G no es trivial**, es decir, $\#Z(G) > 1$ o, equivalentemente, $Z(G) \neq \{1_G\}$.

(IV) Probar que existe H subgrupo normal de G con $\#H = p^{k-1}$. (Sugerencia: Demostrar por inducción sobre k).

Ejercicio I.6.57 (Teorema de Cauchy (Grupos no abelianos)). Sea $(G, \bullet)$ un grupo no abeliano y finito y $p \in \mathbb{N}_{\geq 1}$, con p primo, tal que $p \mid \#G$. Entonces existe $a \in G$ con $O(a) = p$.
Razonamos por reducción al absurdo y suponemos que no existe $a \in G$ con $O(a) = p$. Dividimos la prueba en los siguientes apartados:

(I) Probar que para todo subgrupo propio H de G se tiene que $p \nmid \#H$ y $p \mid (G : H)$.

(II) Probar que existe $g \in G$ con $\#(c\ell(g)) > 1$.

(III) Elegimos representantes $g_1, g_2, \ldots, g_k$ representantes de las clases de conjugación no triviales, probar que

$$\#G = \sum_{c\ell(x) \in G/R} \#c\ell(x) = \#Z(G) + \sum_{i=1}^{k} \#(G : C(g_i)).$$

(IV) Deducir que $p \mid \#(Z(G))$ y llegar a contradicción.

Ejercicio I.6.58 (Grupos de orden pq). Sean p y q primos distintos con $p < q$ y con $p \nmid (q-1)$, equivalentemente, $q \not\equiv 1 \mod p$. El objetivo es probar que todos los grupos de orden pq son isomorfos a C_{pq}.
Sea G un grupo de orden pq, descomponemos la demostración en los siguientes pasos:

(I) Probar, empleando el teorema de Cauchy, que existen $a, b \in G$ con $O(a) = p$ y $O(b) = q$.

(II) Probar que $< b >$ es el único subgrupo de orden q de G.

(III) Probar que $O(aba^{-1}) = q$ y que $aba^{-1} = b^k$.

(IV) Probar que $k^p \equiv 1 \mod q$.

(V) Probar que k tiene orden 1 en $U(\mathbb{Z}/q\mathbb{Z})$.*(Pista: Usar que $p \nmid (q-1)$).*

(VI) Deducir que $ab = ba$ y concluir que $G =< ab >$.

(VII) ¿Cuántos grupos no isomorfos hay de orden 15? ¿y de orden 35? ¿y de orden 39?

(VIII) ¿Podemos obtener información sobre los grupos de orden 21 usando este resultado anterior?

Orden	Grupos Abelianos	Grafo de ciclos	Grupos No Abelianos	Grafo de ciclos
1	C_1 (Grupo trivial)		-	-
2	C_2		-	-
3	C_3		-	-
4	C_4 Subgrupos propios: C_2 Orden de los elementos: 1, 2, 4($\times$2)		-	-
	$K_4 = C_2 \times C_2$ **(Grupo de Klein)** Subgrupos propios: $C_2(\times 3)$ Orden de los elementos: 1, 2($\times$3)		-	-
5	C_5		-	-
6	C_6 Subgrupos propios: C_2, C_3 Orden de los elementos: 1, 2, 3($\times$2), 6($\times$2)		D_3 Subgrupos propios: $C_2(\times 3), C_3$ Orden de los elementos: 1, 2($\times$3), 3($\times$2)	
7	C_7		-	-
8	C_8 Subgrupos propios: C_2, C_4 Orden de los elementos: 1, 2, 4($\times$2), 8($\times$4)		D_4 Subgrupos propios: $C_2(\times 5), C_4, K_4(\times 2)$ Orden de los elementos: 1, 2($\times$5), 4($\times$2)	
	$C_4 \times C_2$ Subgrupos propios: $C_2(\times 3), C_4(\times 2), K_4$ Orden de los elementos: 1, 2($\times$3), 4($\times$4)		Q_8 **(Cuaterniones)** Subgrupos propios: $C_2, C_4(\times 3)$ Orden de los elementos: 1, 2, 4($\times$6)	
	$C_2 \times C_2 \times C_2$ Subgrupos propios: $C_2(\times 7), K_4(\times 7)$ Orden de los elementos: 1, 2($\times$7)		-	-
9	C_9 Subgrupos propios: C_3 Orden de los elementos: 1, 3($\times$2),9($\times$6)		-	-
	$C_3 \times C_3$ Subgrupos propios: $C_3(\times 4)$ Orden de los elementos: 1, 3($\times$8)		-	-
10	C_{10} Subgrupos propios: C_2, C_5 Orden de los elementos: 1, 2, 5($\times$4), 10($\times$4)		D_5 Subgrupos propios: $C_2(\times 5), C_5$ Orden de los elementos: 1, 2($\times$5), 5($\times$4)	
11	C_{11}		-	-
12	C_{12} Subgr. prop.: C_2, C_3, C_4, C_6 Órdenes: 1, 2, 3($\times$2), 4($\times$2), 6($\times$2) 12($\times$4)		D_6 Subgr. prop.: $C_2(\times 7), C_3, K_4(\times 3), D_3(\times 2), C_6$ Órdenes: 1, 2($\times$7), 3($\times$2), 6($\times$2)	
	$C_3 \times C_2 \times C_2$ Subgr. prop.: $C_2(\times 3), C_3, K_4, C_6(\times 3)$ Órdenes: 1, 2($\times$3), 3($\times$2), 6($\times$6)		A_4 Subgr. prop.: $C_2(\times 3)$, $C_3(\times 4)$, K_4 Órdenes: 1, 2($\times$3), 3($\times$8)	
	-	-	Q_{12} Subgr. prop.: C_2, C_3, $C_4(\times 3)$, C_6 Órdenes: 1, 2, 3($\times$2), 4($\times$6), 6($\times$2)	
13	C_{13}		-	-
14	C_{14} Subgrupos propios: C_2, C_7 Orden de los elementos: 1, 2, 7($\times$6), 14($\times$6)		D_7 Subgrupos propios: $C_2(\times 7), C_7$ Orden de los elementos: 1, 2($\times$7), 7($\times$6)	
15	C_{15}		-	-

Tabla I.1: Clasificación de grupos hasta orden 15

II. Introducción a la teoría de anillos

II.1 Nociones Básicas: Anillos y subanillos

Definición II.1.1 Sean R un conjunto no vacío, $+,\cdot : R\times R\to R$ dos operaciones (binarias e internas), decimos que $(R,+,\cdot)$ es un **anillo** si:

(R.I) $(R,+)$ es un **grupo abeliano**.

(R.II) $(R,\cdot)$ es un **semigrupo**, es decir, $\cdot$ satisface la **propiedad asociativa**:
para todos $a,b,c\in R$ se tiene que $a\cdot(b\cdot c)=(a\cdot b)\cdot c$.

(R.III) Se cumple la **propiedad distributiva**: para todos $a,b,c\in R$ se tiene que
$$a\cdot(b+c)=a\cdot b+a\cdot c,$$
$$(a+b)\cdot c=a\cdot c+b\cdot c.$$

Definición II.1.2 Sea $(R,+,\cdot)$ un **anillo** decimos que:

(R.C) $(R,+,\cdot)$ es un **anillo conmutativo** si la operación $\cdot$ es conmutativa, es decir, para todos $a,b\in R$ se tiene que $a\cdot b=b\cdot a$.

(R.U) $(R,+,\cdot)$ es un **anillo unitario** si existe el elemento neutro para la operación $\cdot$, es decir, $(R,\cdot)$ es un **monoide**:
existe $1_R\in R$ tal que para todo $a\in R$ tenemos que $a\cdot 1_R=1_R\cdot a=a$.

Observación II.1.3 ¡Ojo! existe cierta discrepancia en la literatura sobre el uso de la **palabra anillo**. Por brevedad, algunos autores emplean la palabra anillo para referirse a anillos unitarios o incluso a anillos conmutativos y unitarios (sobre todo en textos de Álgebra Conmutativa). En estas notas distinguiremos en cada caso con que tipo de anillo estamos trabajando: *anillo, anillo unitario, anillo conmutativo, anillo conmutativo y unitario.*

Imagen de cabecera: Visualización de los números algebraicos en el plano complejo. Los colores indican el grado más bajo del polinomio de $\mathbb{Z}[x]$ que se anula en el punto (rojo=1(racionales), verde=2, azul=3, amarillo=4, etc.). El tamaño de los puntos se hace más pequeño al aumentar la magnitud de los coeficientes de dicho polinomio. La vista muestra los enteros 0, 1 y 2 en la parte inferior e i en la parte superior izquierda. Imagen creada por Stephen J. Brooks con Licencia - CC BY 3.0 (via en.wikipedia).

Ejemplos II.1.4 (1) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ y $(\mathbb{C},+,\cdot)$ son anillos conmutativos y unitarios.
(2) Para todo $n\in\mathbb{N}_{\geq 1}$ tenemos que $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ es un anillo conmutativo y unitario (ver Ejercicio I.1.6).
(3) $(\mathbb{Z}[x],+,\cdot)$, $(\mathbb{Q}[x],+,\cdot)$, $(\mathbb{R}[x],+,\cdot)$ son anillos conmutativos y unitarios. (ver Sección II.6).
(4) $(\mathrm{Mat}_{n\times n}(\mathbb{Z}),+,\cdot)$ $(\mathrm{Mat}_{n\times n}(\mathbb{Q}),+,\cdot)$ $(\mathrm{Mat}_{n\times n}(\mathbb{R}),+,\cdot)$ $(\mathrm{Mat}_{n\times n}(\mathbb{C}),+,\cdot)$ $(\mathrm{Mat}_{n\times n}(\mathbb{Z}/m\mathbb{Z}),+,\cdot)$ son anillos unitarios no conmutativos.
(5) $(2\mathbb{Z},+,\cdot)$ es un anillo conmutativo no unitario.

Vamos a definir de un modo general diversas nociones que se conocen en el caso particular del anillo de los número enteros o de los anillos de matrices.

Definición II.1.5 Sea $(R,+,\cdot)$ un anillo unitario y $a\in R$, decimos que a **es una unidad de** R si a tiene inverso para el producto, es decir, si existe $b\in R$ tal que $a\cdot b=b\cdot a=1_R$. El conjunto de todas las unidades de R lo denotamos por $U(R)$.

Observación II.1.6 Si $(R,+,\cdot)$ es un anillo unitario, se tiene que $U(R)\neq\emptyset$ porque $1_R\in U(R)$ dado que $1_R\cdot 1_R=1_R\cdot 1_R=1_R$, es decir, 1_R es su propio inverso.

Ejemplos II.1.7 (1) En el anillo de los enteros $(\mathbb{Z},+,\cdot)$ tenemos que $U(\mathbb{Z})=\{-1,1\}$.
(2) En el anillo de los números reales $(\mathbb{R},+,\cdot)$ tenemos que $U(\mathbb{R})=\mathbb{R}\backslash\{0\}$.
(3) En el Ejercicio I.1.7, se probó que

$$U(\mathbb{Z}/n\mathbb{Z})=\{a\in\mathbb{Z}/n\mathbb{Z}\ :\ \text{m.c.d.}\,(a,n)=1\}.$$

Definición II.1.8 Sea $(R,+,\cdot)$ un anillo conmutativo y $a,b\in R$ decimos que a **divide a** b (o equivalentemente a **es divisor de** b o b **es múltiplo de** a) cuando existe $c\in R$ tal que $b=a\cdot c$. En el caso de que se verifique la propiedad escribimos $a\mid b$ y si no se satisface escribimos $a\nmid b$.

Ejemplo II.1.9 Estas nociones de múltiplos y divisores coinciden con las conocidas para los números enteros, ver el apéndice correspondiente. Sin embargo pueden dar lugar a resultados que van en contra de la intuición cuando se trata de otros anillos. Por ejemplo, en $(\mathbb{Z}/12\mathbb{Z})$ tenemos que $5\mid 7$ porque $5\cdot 11\equiv 7\,(\text{mód }12)$.

Definición II.1.10 Sea $(R,+,\cdot)$ un anillo conmutativo y $a\in R$ decimos que a **es un divisor del cero** cuando existe $c\in R$ con $c\neq 0_R$ tal que $a\cdot c=0_R$.

¡Atención! De acuerdo con las definiciones anteriores, todo elemento $a\in R$ divide a cero (porque $0\cdot a=0$) pero no todo elemento es divisor del cero.

Ejemplo II.1.11 En $(\mathbb{Z}/6\mathbb{Z},+,\cdot)$ tenemos que $0|0$ porque $0=0\cdot 0$, $1|0$ porque $0=1\cdot 0$, $2|0$ porque $0=2\cdot 0$, $3|0$ porque $0=3\cdot 0$, $4|0$ porque $0=4\cdot 0$, $5|0$ porque $0=5\cdot 0$ todos los elementos dividen a 0. Sin embargo sólo $0,2,3,4$ son **divisores de cero** en $\mathbb{Z}/6\mathbb{Z}$ porque si miramos el producto de cada elemento por los elementos no nulos tenemos que:

$1\cdot 1=1$	$1\cdot 2=2$	$1\cdot 2=2$	$1\cdot 4=4$	$1\cdot 5=5$	(1 no es divisor de cero)
$2\cdot 1=2$	$2\cdot 2=4$	$\mathbf{2\cdot 3=0}$	$2\cdot 4=2$	$2\cdot 5=4$	(2 es divisor de cero)
$3\cdot 1=3$	$\mathbf{3\cdot 2=0}$	$3\cdot 3=3$	$\mathbf{3\cdot 4=0}$	$3\cdot 5=3$	(3 es divisor de cero)
$4\cdot 1=4$	$4\cdot 2=2$	$\mathbf{4\cdot 3=0}$	$4\cdot 4=4$	$4\cdot 5=2$	(4 es divisor de cero)
$5\cdot 1=5$	$5\cdot 2=4$	$5\cdot 3=3$	$5\cdot 4=2$	$5\cdot 5=1$	(5 no es divisor de cero)

Definición II.1.12 Sea $(R,+,\cdot)$ un anillo unitario y $a \in R$, se dice que:
(A) a es **nilpotente** si existe $n \in \mathbb{N}_{\geq 1}$ tal que $a^n = 0_R$.
(B) a es **idempotente** si $a^2 = a$.

Ejemplo II.1.13 (1) En $(\mathbb{Z}/12\mathbb{Z},+,\cdot)$ comprobamos que:

Los elementos nilpotentes son 0 y 6.

Los elementos idempotente son 0, 1, 4 y 9.

(2) En $(\mathrm{Mat}_{3\times 3}(\mathbb{Z}),+,\cdot)$ consideramos las matrices:

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 2 & -2 & -4 \\ -1 & 3 & 4 \\ 1 & -2 & -3 \end{pmatrix}.$$

La matriz A es nilpotente porque $A^3 = 0$ y la matriz B es idempotente porque $B^2 = B$.

Resumimos algunas propiedades elementales que emplearemos continuamente cuando trabajemos con anillos.

Propiedades II.1.14 — Reglas de multiplicación. Sea $(R,+,\cdot)$ un anillo. Entonces:
(I) Para todo $a \in R$ se tiene que $a \cdot 0_R = 0_R \cdot a = 0_R$.
(II) Para todos $a,b \in R$ se tiene que $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.
(III) Para todos $a,b \in R$ se tiene que $(-a) \cdot (-b) = a \cdot b$.
(IV) Para todo $a \in R$ y todo $n \in \mathbb{Z}$ se tiene que $n \cdot (-a) = (-n) \cdot a = -(n \cdot a)$.
(V) Para todos $a,b \in R$ y todo $m \in \mathbb{Z}$ se tiene que $m(a \cdot b) = (m \cdot a) \cdot b = a \cdot (m \cdot b)$.
(VI) Para todos $a,b \in R$ y todos $m,n \in \mathbb{Z}$ se tiene que $(ma) \cdot (nb) = (mn)(a \cdot b)$.

Propiedades II.1.15 — anillos unitarios. Sea $(R,+,\cdot)$ un anillo unitario. Entonces:
(I) El elemento neutro para el producto de R es único.
(II) Para todo $a \in R$ se tiene que $a \cdot (-1_R) = (-1_R) \cdot a = -a$.
(III) Se tiene que $(-1_R) \cdot (-1_R) = 1_R$.
(IV) Si $a \in U(R)$, entonces su inverso es único (lo denotamos por a^{-1}).
(V) $(U(R),\cdot)$ es un grupo.

De manera natural definimos la noción de subanillo.

Definición II.1.16 Sea $(R,+,\bullet)$ un anillo decimos que un subconjunto S no vacío de R es un **subanillo** si al restringir las operaciones binarias $+,\bullet$ a S tenemos que $(S,+_{|S},\bullet_{|S})$ es un anillo. *(Abusando de la notación hemos escrito $+_{|S}$, $\bullet_{|S}$ en lugar de $+_{|S\times S}$, $\bullet_{|S\times S}$)*

Al igual que ocurría para subgrupos tenemos un test de caracterización de subanillos que nos permite comprobar de una forma ágil cuando un subconjunto de R es un subanillo.

Proposición II.1.17 — (Test de caracterización de subanillos). Sea $(R,+,\bullet)$ un anillo y S un subconjunto no vacío de R entonces son equivalentes:
(I) S es un subanillo de R.
(II) Para todos $a,b \in S$ se cumple $\begin{cases} \text{(SR. I)} & a-b \in S, \\ \text{(SR. II)} & a \bullet b \in S. \end{cases}$

Demostración. (I)$\Rightarrow$ (II) Por hipótesis $(S,+_{|S},\bullet_{|S})$ es un anillo. Por tanto, dados $a,b \in S$ como $(S,+_{|S})$ es un grupo tenemos que $a,-b \in S$ y como $+_{|S} : S \times S \to S$ es una operación binaria interna tenemos que $a-b \in S$, es decir, se satisface (SR.I). Como $\bullet_{|S} : S \times S \to S$ es una operación binaria interna dados $a,b \in S$ tenemos que $a \bullet b \in S$, es decir, se cumple (SR.II).

(II)⇒ (I) Empleando la condición (SR.I) deducimos del **test de caracterización de subgrupos** que S es un subgrupo de $(R,+)$, por tanto, $+_{|S}: S\times S\to S$ es una operación binaria interna que satisface la propiedad asociativa, existencia de elemento neutro y de elemento inverso. Además, como $(R,+)$ es un grupo abeliano deducimos que $(S,+_{|S})$ es un grupo abeliano, es decir, se verifica (R.I).

Por (SR.II) vemos que $\bullet_{|S}: S\times S\to S$ es una operación binaria interna y como $\bullet: R\times R\to R$ satisface la propiedad asociativa $(S,\bullet_{|S})$ es un semigrupo, luego se satisface (R.II).

Finalmente como la propiedad distributiva se verifica en $(R,+,\bullet)$ se cumple también en $(S,+_{|S},\bullet_{|S})$ y concluimos que la propiedad (R.III) es cierta y que $(S,+_{|S},\bullet_{|S})$ es un anillo. ■

Ejemplos II.1.18 (1) $\mathbb{Z}[x]$ es subanillo de $(\mathbb{Q}[x],+,\cdot)$.

(2) $\mathbb{Z}[i]=\{a+bi\ :\ a,b\in\mathbb{Z}\}$ **(enteros de Gauss)** es subanillo de $(\mathbb{C},+,\cdot)$.

(3) El conjunto de las matrices diagonales $D_2(\mathbb{Z})$ es subanillo de $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$. Sin embargo, el conjunto de las matrices simétricas $S_2(\mathbb{Z})$ es un subgrupo de $(\mathrm{Mat}_{2\times 2}(\mathbb{Z}),+)$ como vimos en el Bloque I, pero no es un subanillo de $(\mathrm{Mat}_{2\times 2}(\mathbb{Z}),+,\cdot)$ porque

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1&1\\1&1\end{pmatrix}=\begin{pmatrix}1&1\\0&0\end{pmatrix}\notin S_2(\mathbb{Z})$$

Ejercicio II.1.19 Dar un ejemplo de un anillo $(R,+,\cdot)$ que no sea ni unitario ni conmutativo.

Ejercicio II.1.20 ¿Para qué valores de $n\in\mathbb{N}_{\geq 1}$ existen divisores del cero no nulos en el anillo $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$?

Ejercicio II.1.21 ¿Qué relación hay entre los elementos nilpotentes y los divisores del cero? ¿Podrías dar un ejemplo de una matriz no nula nilpotente en $\mathrm{Mat}_{2\times 2}(\mathbb{R})$? ¿y de una matriz nilpotente con todas sus entradas no nulas idempotente?

Ejercicio II.1.22 Probar las reglas de multiplicación de las Propiedades II.1.14.

Ejercicio II.1.23 Probar la Propiedades II.1.15 de los anillos unitarios.

Ejercicio II.1.24 (Producto cartesiano de anillos). Sean $R_1,R_2,\ldots,R_n$ anillos. Sobre $R_1\times R_2\times\cdots\times R_n$ (el producto cartesiano) definimos la suma y el producto componente a componente:

$$(a_1,a_2,\ldots,a_n)\boxplus(b_1,b_2,\ldots,b_n):=(a_1+b_1,a_2+b_2,\ldots,a_n+b_n),$$
$$(a_1,a_2,\ldots,a_n)\boxdot(b_1,b_2,\ldots,b_n):=(a_1b_1,a_2b_2,\ldots,a_nb_n).$$

Probar que $(R_1\times R_2\times\cdots\times R_n,+,\cdot)$ es un anillo.

Ejercicio II.1.25 Dado R es un anillo unitario, probar que $S=\{n\cdot 1_R : n\in Z\}$ es un subanillo de R y que $S\subseteq T$ para cualquier subanillo T de R con $1_R\in T$.

Ejercicio II.1.26 Determinar el menor subanillo de $\mathbb{Q}$ que contiene a $1/2$.

Ejercicio II.1.27 Determinar las unidades de los anillos $Mat_{n\times n}(\mathbb{Z})$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$ y $\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$ **(Enteros de Gauss)**.

Ejercicio II.1.28 Probar que $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} : a,b \in \mathbb{Z}\}$ es un subanillo de $\mathbb{R}$ que posee infinitas unidades.

Ejercicio II.1.29 Probar que si a,b son elementos de un anillo unitario R y a es unidad, la ecuación $ax = b$ tiene solución única y poner algún ejemplo para probar que, cuando a no es unidad, esta ecuación puede no tener solución o tener más de una.

Ejercicio II.1.30 Probar que si $R_1, R_2, \ldots, R_m$ son anillos conmutativos y unitarios se cumple que

$$U(R_1 \times R_2 \times \cdots \times R_m) = U(R_1) \times U(R_2) \times \cdots \times U(R_m). \quad \text{(Ver Ejercicio II.1.24)}$$

Ejercicio II.1.31 Dado $(R,+,\cdot)$ un anillo unitario (no necesariamente conmutativo) y $a,b \in R$ tales que $a \cdot b = 1_R$ y que a no es divisor de 0, probar que $b \cdot a = 1_R$.

Ejercicio II.1.32 Dado $(R,+,\cdot)$ un anillo conmutativo y unitario y $u \in U(R)$, probar que u divide a cada elemento de R.

Ejercicio II.1.33 Probar que en el anillo $Mat_{2\times 2}(\mathbb{Z})$ existen elementos A,B tales que $AB = 0$ y $BA \neq 0$

Ejercicio II.1.34 (Subanillos de $\mathbb{Z}$). Sea A un subconjunto no vacío de $\mathbb{Z}$. Probar que son equivalentes:
(I) A es un subanillo de $(\mathbb{Z},+)$.
(II) Existe $n \in \mathbb{N}$ tal que $A = n\mathbb{Z}$.
(*Nota:* Emplear el Ejercicio I.2.17)

II.2 Ideales, anillo cociente y característica

II.2.1 Ideales

Los **subgrupos normales** juegan un papel especial en la teoría de grupos, puesto que permiten la construcción del grupo cociente. Del mismo modo, disponemos de una noción análoga en la teoría de anillos: los **ideales** que nos van a permitir construir el anillo cociente.

Definición II.2.1 Sea $(R,+,\cdot)$ un anillo e I **es un subanillo de** R se dice que:

(A) I es **un ideal por la izquierda de** R si para todo $r \in R$ y todo $x \in I$ tal que $r \cdot x \in I$.

(B) I es **un ideal por la derecha de** R si para todo $r \in R$ y todo $x \in I$ tal que $x \cdot r \in I$.

Si I satisface (A) y (B) decimos que I es un **ideal bilatero** o simplemente un **ideal**.

Por tanto, un ideal es un subanillo que 'absorbe' los elementos de R.

Proposición II.2.2 — Test de caracterización de ideales. Sea $(R,+,\cdot)$ un anillo e I un subconjunto no vacío de de R. Entonces:

$$I \text{ es un ideal de } R \Leftrightarrow \text{ para todos } x,y \in I \text{ y todo } r \in R \text{ se tiene que } \begin{cases} (1) & x-y \in I, \\ (2) & r\cdot x \in I, \\ (3) & x\cdot r \in I. \end{cases}$$

Demostración. El resultado se prueba deforma directa empleando el **Test de caracterización de subanillos** (Proposición II.1.17) y la definición de ideal. ■

Ejemplos II.2.3 (1) $\{0_R\}$ y R son siempre ideales de R.
(2) Para todo $n \in \mathbb{N}$ tenemos que $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$.
(3) Si $(R,+,\cdot)$ es un anillo conmutativo y $a \in R$ el conjunto $\{r \cdot a : r \in R\}$ es un ideal.

Al igual que para subgrupos normales, vamos a estudiar las operaciones elementales entre ideales.

Proposición II.2.4 Sea $(R,+,\cdot)$ un anillo y $\{I_j\}_{j\in J}$ una familia de ideales. Entonces:

$$\cap_{j\in J} I_j, \text{ es un ideal de } R.$$

Demostración. Dados $x,y \in \cap_{j\in J} I_j$ y $r \in R$, por tanto $x,y \in I_j$ y como cada I_j es un ideal, por el **Test de caracterización de ideales** (Proposición II.2.2) tenemos que para todo $j \in J$ se cumple que $x-y \in I_j$, $r\cdot x \in I_j$, $x\cdot r \in I_j$. En consecuencia, $x-y \in \cap_{j\in J} I_j$, $r\cdot x \in \cap_{j\in J} I_j$, $x\cdot r \in \cap_{j\in J} I_j$ y, de nuevo, empleando el **Test de caracterización de ideales** concluimos que $\cap_{j\in J} I_j$ es un ideal de R. ■

Definición II.2.5 Sea $(R,+,\cdot)$ un anillo y X un subconjunto de R, llamamos **ideal generado por** X a la intersección de todos los ideales que contienen a X y lo denotamos por

$$(X) := \bigcap_{I_j \text{ ideal}, X\subseteq I_j} I_j.$$

Observación II.2.6 (X) es un ideal, por la Proposición II.2.4, que contiene a X y, además, si J es un ideal y $X \subseteq J$, entonces $(X) \subseteq J$, es decir, (X) es el ideal más pequeño que contiene al subconjunto X.

Notación II.2.7 Emplearemos la notación abreviada aditiva y multiplicativa al igual que en grupos, ver Notación I.1.4.

Proposición II.2.8 Sea $(R,+,\cdot)$ un anillo y X un subconjunto no vacío de R, entonces:

$$(X) = \left\{ \sum_{i=1}^{m} (n_i x_i + r_i x_i + x_i s_i + r_i x_i s_i) \ : \ m \in \mathbb{N}_{\geq 1},\ s_i, r_i \in R,\ x_i \in X,\ n_i \in \mathbb{Z} \right\}.$$

Demostración. Llamamos A a la expresión de la derecha de esta igualdad. Como (X) es un ideal tiene que contiene a X por las propiedades (1), (2) y (3), ver Proposición II.2.2, contiene a todos los elementos de la forma: nx, rx, xs y rxs con $r,s \in R$, $x \in X$ y $n \in \mathbb{Z}$. Por tanto, como todo ideal es un subgrupo, contiene a todas las sumas de elementos de ese tipo y deducimos que $A \subseteq (X)$.
Empleando la Proposición II.2.2, comprobamos que A es un ideal y como $X \subseteq A$ y concluimos que $(X) \subseteq A$. ■

Observación II.2.9 La descripción de (X) de la Proposición II.2.8 se puede simplificar si el anillo R satisface más propiedades. Si R es un **anillo unitario** y X es un subconjunto no vacío de R:

$$(X) = \left\{ \sum_{i=1}^{m} r_i x_i s_i \ : \ m \in \mathbb{N}_{\geq 1},\ s_i, r_i \in R,\ x_i \in X \right\}.$$

Si R es un **anillo conmutativo y unitario** y X es un subconjunto no vacío de R:

$$(X) = \left\{ \sum_{i=1}^{m} r_i x_i \ : \ m \in \mathbb{N}_{\geq 1},\ r_i \in R,\ x_i \in X \right\}.$$

En particular, si R es un **anillo conmutativo y unitario** y si $X = \{a\}$ con $a \in R$ tenemos que $(\{a\}) = \{ra : r \in R\}$.

Abusando de la notación cuando un ideal esté generado por un número finito de elementos $\{a_1, a_2, \ldots, a_r\}$ y lo denotaremos por $(a_1, a_2, \ldots, a_r)$ en lugar de $(\{a_1, a_2, \ldots, a_r\})$.

En general la unión de dos ideales no es un ideal pero podemos considerar el ideal generado por la unión y describirlo en términos de la suma de ideales.

Definición II.2.10 Sea $(R, +, \cdot)$ un anillo, I, J ideales de R, entonces llamamos **suma de los ideales I y J** a

$$I + J := \{x + y : x \in I\, y \in J\}.$$

Proposición II.2.11 Sea $(R, +, \cdot)$ un anillo, I, J ideales de R, entonces el ideal generado por la unión de I y J coincide con la suma de I y J, es decir,

$$(I \cup J) = I + J.$$

Demostración. Dados $x \in I$ y $y \in J$ tenemos que $x, y \in I \cup J \subseteq (I \cup J)$ y, como $(I \cup J)$ es un ideal, $x + y \in (I \cup J)$. En consecuencia, se cumple que $I + J \subseteq (I \cup J)$. Ahora veamos que $I + J$ es un ideal que contiene a $I \cup J$.
Como $0_R \in I$ y $0_R \in J$ tenemos que $I, J \subseteq I + J$ y, por tanto, $I \cup J \subseteq I + J$. Dados $a_1, a_2 \in I + J$ y $r \in R$ tenemos que $a_1 = x_1 + y_1$ y $a_2 = x_2 + y_2$ con $x_1, x_2 \in I$ e $y_1, y_2 \in J$. Como I y J son ideales, por la Proposición II.2.2, se tiene que

$$x_1 - x_2 \in I, \quad rx_1 \in I, \quad x_1 r \in I, \quad y_1 - y_2 \in J, \quad ry_1 \in J, \qquad y_1 r \in J.$$

Por consiguiente, se tiene que $a_1 - a_2 = (x_1 - x_2) + (y_1 - y_2) \in I + J$, $ra_1 = rx_1 + ry_1 \in I + J$, y $a_1 r = x_1 r + y_1 r \in I + J$, luego $I + J$ es un ideal (Proposición II.2.2). Como $I + J$ es un ideal que contiene a $I \cup J$ concluimos que $(I \cup J) \subseteq I + J$ y deducimos que $I + J = (I \cup J)$. ■

II.2.2 Anillo cociente

Dado $(R, +, \cdot)$ un anillo, $(R, +)$ es un grupo conmutativo y, por tanto, todo subgrupo de R es un subgrupo normal. En particular, si I es un ideal como es **subanillo tenemos que $(I, +)$ es subgrupo normal**, es decir, $(I, +) \lhd (R, +)$. De esta forma, podemos considerar:

$$R/I := \{a + I \ : \ a \in R\} \qquad (a + I) + (b + I) := (a + b) + I.$$

La teoría de grupos garantiza, ver Teorema I.5.28, que $(R/I, +)$ es un grupo y como $(R, +)$ es abeliano el cociente también.

Veamos como dotar de estructura de anillo al grupo abeliano $(R/I, +)$.

Teorema II.2.12 (Anillo Cociente). Sea $(R, +, \cdot)$ un anillo e I un ideal de R, entonces el grupo abeliano $(R/I, +)$ tiene estructura de anillo respecto del producto definido para todos $a, b \in R$ por

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

Demostración. En primer lugar veamos que la operación binaria interna $\cdot$ está **bien definida**. Si $a_1+I=a_2+I$ y $b_1+I=b_2+I$ tenemos que $a_1-a_2\in I$ y $b_1-b_2\in I$. Como I es un ideal $(a_1-a_2)b_1\in I$ y $a_2(b_1-b_2)\in I$. Por tanto, empleando la propiedad distributiva, se verifica que

$$a_1b_1-a_2b_2=a_1b_1-a_2b_1+a_2b_1-a_2b_2=(a_1-a_2)b_1+a_2(b_1-b_2)\in I,$$

de donde deducimos que $(a_1b_1)+I=(a_2b_2)+I$ y, por esta razón, el producto está bien definido en R/I. Finalmente, el producto es asociativo en R/I por ser el producto asociativo en R y la propiedad distributiva se cumple en R/I por cumplirse en R. Por consiguiente, $(R/I,+,\cdot)$ es un anillo. ■

Observación II.2.13 Si $(R,+,\cdot)$ es un anillo unitario, entonces 1_R+I es el elemento neutro de R/I porque $a\in R$ por

$$(a+I)\cdot(1_R+I)=(a1_R)+I\overset{R\text{ unitario}}{=}a+I\overset{R\text{ unitario}}{=}(1_Ra)+I=(1_R+I)\cdot(a+I).$$

Si $(R,+,\cdot)$ es conmutativo, entonces R/I conmutativo porque para todos $a,b\in R$ por

$$(a+I)\cdot(b+I)=(ab)+I\overset{R\text{ conmutativo}}{=}(ba)+I=(b+I)\cdot(a+I).$$

Ejemplo II.2.14 Consideramos el anillo de los enteros de Gauss $R=\mathbb{Z}[i]=\{a+bi:a,b\in\mathbb{Z}\}$ y el ideal $I=(2-i)$. ¿Cuántos elementos hay en R/I?

Recordamos que $x+I=y+I$ si y solo si $x-y\in I$, ver Notación I.5.4 y Propiedades I.5.8.

Como $\mathbb{Z}[i]$ es un anillo conmutativo y unitario, por la Observación II.2.9, tenemos que

$$I=(2-i)=\{(a+bi)(2-i):a,b\in\mathbb{Z}\}$$

Por ese motivo, como $2-i\in I$ deducimos que la clase de 2 y la de i son iguales, es decir, $i+I=2+I$. Empleando la misma técnica vemos que para todos $a,b\in\mathbb{Z}$ la clase de $(a+bi)$ y $(a+2b)$ coinciden porque

$$a+2b-(a+bi)=b(2-i)\in I.$$

De este modo hemos probado que siempre podemos elegir un representante de la clase $(a+bi)+I$ de R/I en $\mathbb{Z}$, es decir, de la forma $c+I$ con $c\in\mathbb{Z}$.

Por último, observamos que 5 puede escribirse como un múltiplo de $(2-i)$, en otras palabras, 5 está en el ideal porque $5=(2+i)(2-i)\in I$ [*]. De aquí, deducimos que dados $c,d\in\mathbb{Z}$ si $d-c\in 5\mathbb{Z}$ tenemos que $d-c\in I$ y, por tanto, $c+I=d+I$. En virtud de esta propiedad concluimos que el representante de una clase de R/I siempre puede elegirse en el conjunto $\{0,1,2,3,4\}$, en otros términos, toda clase es igual a alguna de las siguientes:

$$0+I,\quad 1+I,\quad 2+I,\quad 3+I,\quad 4+I.$$

Finalmente, comprobamos que estás cinco clases son diferentes, porque $e+I=f+I$ con $e,f\in\mathbb{Z}$ si y solamente si $e-f=(a+bi)(2-i)$ para algunos $a,b\in\mathbb{Z}$, dicho de otro modo $e+I=f+I$ si y solamente si $e-f=2a+b+i(2b-a)$. Igualando la parte real y la imaginaria, se tiene que $e+I=f+I$ si y solamente si $e-f=2a+b$ y $2b-a=0$ si y sólo si $e-f=5b$ y $2b=a$ si y sólo si $e-f\in 5\mathbb{Z}$. De esta forma, se cumple que:

$$\mathbb{Z}[i]/(2-i)=R/I=\{0+I,\quad 1+I,\quad 2+I,\quad 3+I,\quad 4+I\}.$$

[*]Escoger el número 5 puede parecer una 'idea feliz' pero lo cierto es que es bastante natural porque ¿cuál es la norma del complejo $(2-i)$? ¿Cuál es la relación entre un complejo, su conjugado y su norma? Si $z\in\mathbb{Z}[i]$ ¿$\bar{z}\in\mathbb{Z}[i]$?

II.2.3 Característica de un anillo

Veamos como definir de forma rigurosa la noción de característica, siguiendo [14].

Definición II.2.15 Sea $(R,+,\cdot)$ un anillo, consideramos el conjunto

$$C=\{n\in\mathbb{N}_{\geq 1} \ : \ nx=0_R \text{ para todo } x\in R\}.$$

Si C es vacío decimos que la **característica de R es 0**, es decir, $\text{car}(R)=0$.
Si C no es vacío decimos que la **característica de R es el mínimo del conjunto** C, es decir, $\text{car}(R)=\text{mín}(C)$.

Determinar la característica de un anillo cualquiera puede ser una tarea complicada. Sin embargo, cuando dicho anillo es unitario el trabajo se simplifica, como muestra el siguiente resultado. En esta situación, la característica es el menor numero de veces que debemos sumar el elemento neutro multiplicativo del anillo, 1_R, con él mismo para obtener el elemento neutro aditivo, 0_R. Si la suma nunca alcanza la unidad aditiva el anillo tiene característica cero.

Teorema II.2.16 (Característica de un anillo unitario). Sea $(R,+,\cdot)$ un anillo unitario y $n\in\mathbb{N}_{\geq 1}$, entonces

$$\begin{aligned}\text{car}(R)=0 &\quad\Leftrightarrow\quad O(1_R)=\infty \quad \text{en} \quad (R,+).\\ \text{car}(R)=n &\quad\Leftrightarrow\quad O(1_R)=n \quad \text{en} \quad (R,+).\end{aligned}$$

Demostración. Consideramos los conjuntos

$$C=\{n\in\mathbb{N}_{\geq 1} \ : \ \forall x\in R, \ \ nx=0_R\} \quad \text{y} \quad B=\{n\in\mathbb{N}_{\geq 1} \ : \ n1_R=0_R\},$$

Observamos que $C\subseteq B$. Si $n\in B$, empleando las reglas de multiplicación del los anillos, ver Proposición II.1.14, para todo $x\in R$ vemos que $nx=n(1_R\cdot x)=(n1_R)\cdot x=0_R\cdot x=0_R$, luego $n\in C$ y deducimos que $C=B$. Por consiguiente, se tiene que

$$\begin{aligned}\text{car}(R)=0 &\quad\Leftrightarrow\quad C=\emptyset \quad\Leftrightarrow\quad B=\emptyset \quad\Leftrightarrow\quad O(1_R)=\infty \quad \text{en} \quad (R,+).\\ \text{car}(R)=n &\quad\Leftrightarrow\quad n=\text{mín}(C) \quad\Leftrightarrow\quad n=\text{mín}(B) \quad\Leftrightarrow\quad O(1_R)=n \quad \text{en} \quad (R,+).\end{aligned}$$

■

Ejemplo II.2.17 (1) $(\mathbb{Z},+,\cdot)$ es un anillo de característica 0.
Como $\mathbb{Z}$ es un anillo unitario podemos aplicar el Teorema II.2.16. Sabemos que $O(1)=\infty$ en $(\mathbb{Z},+)$ porque $n1\neq 0$ para todo $n\in\mathbb{N}_{\geq 1}$, luego $\text{car}(\mathbb{Z})=0$.

(2) Para $m\in\mathbb{N}_{\geq 1}$, se tiene que $(\mathbb{Z}/m\mathbb{Z},+,\cdot)$ es un anillo de característica m.
Como $\mathbb{Z}/m\mathbb{Z}$ es un anillo unitario podemos aplicar el Teorema II.2.16. Sabemos que $O(1)=m$ en $(\mathbb{Z}/m\mathbb{Z},+)$ porque $m1=0$, luego $\text{car}(\mathbb{Z}/m\mathbb{Z})=m$.

(3) $((\mathbb{Z}/2\mathbb{Z})[x],+,\cdot)$ es un anillo infinito de característica 2.
Como $\mathbb{Z}/2\mathbb{Z}[x]$ es un anillo unitario podemos aplicar el Teorema II.2.16. El elemento neutro para el producto en $\mathbb{Z}/2\mathbb{Z}[x]$ es el polinomio constante 1. Sabemos que $O(1)=2$ en $(\mathbb{Z}/2\mathbb{Z}[x],+)$ porque $1+1=2\cdot 1=0$, luego $\text{car}(\mathbb{Z}/2\mathbb{Z}[x])=2$.

(4) La característica del anillo producto $R=\mathbb{Z}/4\mathbb{Z}\times 4\mathbb{Z}$, ver Ejercicio II.1.24, es $\text{car}(R)=0$.
Como R es un anillo que no es unitario no podemos aplicar el Teorema II.2.16. Observamos que tomando $a=(0,4)$ para todo $n\in\mathbb{N}_{\geq 1}$ se tiene que $na=(0,4n)\neq(0,0)$, es decir, el orden aditivo de a es infinito y, por tanto, $\text{car}(R)=0$.

Ejercicio II.2.18 ¿Podrías dar un ejemplo de un subanillo que no sea un ideal?

Ejercicio II.2.19 En los siguientes casos describir los elementos del ideal I del anillo R:

(I) $I=(2,x^2)$, $R=\mathbb{Z}[x]$, $R=\mathbb{Q}[x]$.

(II) $I=(2)$, $I=(1+i)$, $R=\mathbb{Z}[i]$.

Ejercicio II.2.20 (Ideales de $\mathbb{Z}$). Sea I un subconjunto no vacío de $\mathbb{Z}$. Probar que son equivalentes:
(I) I es un ideal de $(\mathbb{Z},+)$.
(II) Existe $n\in\mathbb{N}$ tal que $I=n\mathbb{Z}$.
(*Nota:* Emplear el Ejercicio I.2.17 y el Ejercicio II.1.34)

Ejercicio II.2.21 Dado $(R,+,\cdot)$ un anillo, I un ideal de R y A un subanillo de R. Probar que:

(I) $A+I=\{a+x : x\in I, a\in A\}$ es un subanillo de R que contiene a I y A.

(II) I es un ideal de $A+I$.

(III) $A\cap I$ es un ideal de A.

Ejercicio II.2.22 (Producto de ideales). Si I, J son ideales de un anillo R probar que

$$IJ=\{a_1b_1+\cdots+a_nb_n : n\in\mathbb{N}, a_i\in I, b_i\in J\}$$

es un ideal de R y que $IJ\subseteq I\cap J$.

Ejercicio II.2.23 Si $R=\mathbb{Z}$, $I=(12)$ y $J=(20)$, determinar enteros a, b, c tales que $(a)=(12)+(20)$, $(b)=(12)\cap(20)$ y $(c)=(12)(20)$.

Ejercicio II.2.24 Si I, J son ideales de un anillo conmutativo y unitario R y $I+J=R$, probar que $IJ=I\cap J$ (ver Ejercicio II.2.22).

Ejercicio II.2.25 Dado un ideal I de un anillo unitario R, probar que si $1_R\in I$, entonces $I=R$.

Ejercicio II.2.26 Dado R un anillo conmutativo y unitario y sean $I_1,I_2,\ldots,I_k$ ideales de R tales que $I_i+I_j=R$ si $i\neq j$. Probar que: $I_i+\cap_{i\neq j}I_j=R$.

Ejercicio II.2.27 Dado $(R,+,\cdot)$ un anillo e I un ideal de R, probar que existe una biyección entre el conjunto de ideales de J de R que contienen a I y los ideales de R/I.

Ejercicio II.2.28 Consideramos $R=\mathrm{Mat}_{2\times2}(\mathbb{Z})$ y $I=\mathrm{Mat}_{2\times2}(3\mathbb{Z})$. ¿Cuántos elementos hay en R/I?

Ejercicio II.2.29 Determinar el número de elementos que posee el anillo $\mathbb{Z}[i]/(3+i)$.

Ejercicio II.2.30 ¿Existe un anillo R con $\mathrm{car}(R)=0$ tal que para todo $x\in R$ existe $n\in\mathbb{N}_{\geq1}$ con $nx=0_R$?

II.3 Homomorfismos de anillos

II.3.1 Nociones básicas

En el primer bloque hemos visto que un modo de obtener información sobre un grupo es examinar su interacción con otros grupos mediante homomorfismos. Esta noción de una aplicación que conserva la estructura algebraica (en este caso las operaciones) se extiende a la teoría anillos de un modo satisfactorio.

Definición II.3.1 Sean R y S anillos y $f : R \to S$ una aplicación, decimos que f es un **homomorfismo de anillos** si se cumplen las siguientes condiciones:

(H.A.I) Para todos $a,b \in R$ tenemos que $f(a+b) = f(a)+f(b)$,

(H.A.II) Para todos $a,b \in R$ tenemos que $f(ab) = f(a)f(b)$.

Ejemplos II.3.2 (1) La aplicación $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ dada para todo $a \in \mathbb{Z}$ por $f(a) = a \bmod n$ es un homomorfismo de anillos sobreyectivo.

(2) La aplicación $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ definida por $f(a) = 4a$ es un homomorfismo de anillos.

(3) Consideramos la aplicación $f : \mathbb{C} \to \mathbb{C}$ dada por $f(z) = \bar{z}$ para todo $z \in \mathbb{C}$. Usando las propiedades de la **conjugación compleja** (SecciónA.3) se puede probar que f es un homomorfismo de anillos.

(4) La aplicación $f : \mathbb{R}[x] \to \mathbb{R}$ que envía cada polinomio en su valor al evaluar en 2021, es decir, $f(P) = P(2021)$ es un homomorfismo de anillos sobreyectivo. De hecho, esto es un caso particular de un resultado más general (ver Corolario II.6.16).

(5) La aplicación $f : \mathbb{C} \to \mathrm{Mat}_{2\times 2}(\mathbb{R})$ dada por $f(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ es un homomorfismo de anillos.

Los homomorfismos de anillos satisfacen propiedades similares a los homomorfismos de grupos. De hecho, como **todo homomorfismo de anillos $f : (R,+,\cdot) \to (S,+,\cdot)$ es un homomorfismo de grupos entre los grupos aditivos** $f : (R,+) \to (S,+)$, podemos considerar su núcleo $\mathrm{Ker} f = f^{-1}(\{0_S\})$ y su imagen $\mathrm{Im} f = f(R)$ y obtener de forma rápida varias de las propiedades listadas a continuación.

Propiedades II.3.3 Sean R y S anillos y $f : R \to S$ un homomorfismo de anillos. Entonces se cumple que:

(I) $f(0_R) = 0_S$.

(II) Si A es un subanillo de R, entonces $f(A)$ es un subanillo de S.

(III) $\mathrm{Im} f = f(R)$ es un subanillo de S.

(IV) Si B es un subanillo de S, entonces $f^{-1}(B)$ es un subanillo de R.

(V) Si I es un ideal de R y f es sobreyectivo entonces $f(I)$ es un ideal de S.

(VI) Si J es un ideal de S, entonces $f^{-1}(J)$ es un ideal de R.

(VII) $\mathrm{Ker} f = f^{-1}(\{0_S\})$ es un ideal de R.

Definición II.3.4 Sean R y S anillos unitarios y $f : R \to S$ un homomorfismo de anillos decimos que f es un **homomorfismo de anillos unitarios** si $f(1_R) = 1_S$.

Definición II.3.5 Sean R y S dos anillos y $f : R \to S$ un homomorfismo de anillos. Si f es un homomorfismo de anillos biyectivo decimos que es un **isomorfismo**,

Propiedades II.3.6 Sean R, S, T tres anillos. Entonces se cumple que:
(I) Si $f : R \to S$ y $g : S \to T$ son homomorfismos de anillos, entonces $g \circ f$ es un homomorfismo de anillos.
(II) Si $f : R \to S$ es un isomorfismo de anillos, entonces $f^{-1} : S \to R$ es isomorfismo de anillos.

Definición II.3.7 Sean R y S dos anillos. Si existe un isomorfismo entre dos anillos R y S diremos que R y S son **anillos isomorfos** y escribiremos $R \approx S$.

Observación II.3.8 Si R, S y T tres anillos. Siempre se cumple que $R \approx R$. Si $R \approx S$, entonces $S \approx R$ (Propiedad II.3.6.(II)). Si $R \approx S$ y $S \approx T$, entonces $R \approx T$ (Propiedad II.3.6.(I))

II.3.2 Teoremas de isomorfía

Podemos extender los teoremas de la Sección I.6.2 al contexto de anillos. Los resultados son idénticos, basta cambiar las palabras grupo, subgrupo y subgrupo normal por anillo, subanillo e ideal, respectivamente.

Lema II.3.9 Sean R y S anillos, $f : R \to S$ un homomorfismo de anillos e I un ideal de R con $I \subseteq \mathrm{Ker} f$, se cumple que:

$$\overline{f} : R/I \to S \text{ dado por } \overline{f}(a+I) = f(a) \text{ para todo } a \in R$$

es un homomorfismo de anillos. Además, $\overline{f}$ es el único homomorfismo de anillos $g : R/I \to S$ tal que $g(a+I) = f(a)$ para todo $a \in R$.

Demostración. Como f es un homomorfismo de anillos, f es, en particular, un homomorfismo de grupos y, como I es un ideal, $(I,+)$ es un subgrupo normal de $(R,+)$ contenido en el $\mathrm{Ker} f$. Por tanto, aplicando el Lema I.6.15, se tiene que $\overline{f} : R/I \to S$ está bien definido, es único y es homomorfismo de grupos, es decir, se cumple (HA.I).
Finalmente, basta observar que por la definición del producto en R/I y como f es homomorfismo de anillos para todos $a, b \in R$ se tiene que

$$\overline{f}((a+I)(b+I)) = \overline{f}((ab)+I) = f(ab) = f(a)f(b) = \overline{f}(a+I)\overline{f}(b+I). \quad \blacksquare$$

Observación II.3.10 Sean R y S anillos unitarios, $f : R \to S$ un homomorfismo de anillos unitarios e I un ideal de R con $I \subseteq \mathrm{Ker} f$, entonces $\overline{f} : R/I \to S$, dada por el Lema anterior, es también un homomorfismo de anillos unitarios porque

$$\overline{f}(1_{R/I}) = \overline{f}(1_R + I) = f(1_R) = 1_S.$$

Teorema II.3.11 (Primer Teorema de Isomorfía). Sean R y S anillos, $f : R \to S$ un homomorfismo de anillos, entonces se cumple que

$$R \Big/ \mathrm{Ker} f \approx \mathrm{Im} f.$$

Demostración. Por el Lema II.3.9 sabemos que $\overline{f} : R/\mathrm{Ker} f \to S$ es un homomorfismo de anillos. Vemos que

$$a \in \mathrm{Ker}\overline{f} \quad \Leftrightarrow \quad \overline{f}(a + \mathrm{Ker} f) = 0_S \quad \Leftrightarrow \quad f(a) = 0_S.$$

Por tanto, se tiene que $a \in \mathrm{Ker}\overline{f}$ si y solamente si $a \in \mathrm{Ker}f$ o, equivalentemente, $a + \mathrm{Ker}f = 0_R + \mathrm{Ker}f = 0_{R/\mathrm{Ker}f}$. Por consiguiente, se cumple que $\overline{f}$ es inyectiva.
Finalmente, observamos que $\mathrm{Im}f = \mathrm{Im}\overline{f}$ y, en consecuencia, $\overline{f} : R/\mathrm{Ker}f \to \mathrm{Im}f$ es un isomorfismo de anillos. ■

Ejemplos II.3.12 (1) Consideramos $f : \mathbb{Q}[x] \to \mathbb{R}$ dada por $f(P) = P(0)$, la evaluación en 0. Comprobamos que f es un homomorfismo de anillo, que la imagen es $\mathrm{Im}f = \mathbb{Q}$ y que el núcleo es $\mathrm{Ker}f = \{P(x) \in \mathbb{Q}[x] \ : \ P(0) = 0\} = (x)$. Por consiguiente, aplicando el Primer Teorema de Isomorfía tenemos que

$$\mathbb{Q}[x] \Big/ (x) \approx \mathbb{Q}.$$

(2) Consideramos $f : \mathrm{Mat}_{2\times 2}(\mathbb{Z}) \to \mathrm{Mat}_{2\times 2}(\mathbb{Z}/7\mathbb{Z})$ el homomorfismo de anillos que envía cada matriz A en la matriz que resulta al tomar clase de sus entradas módulo 7, es decir, está dado por

$$f\left(\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}\right) = \begin{pmatrix} [a_{1,1}]_7 & [a_{1,2}]_7 \\ [a_{2,1}]_7 & [a_{2,2}]_7 \end{pmatrix}.$$

Comprobamos que f es un homomorfismo de anillos, que f es sobreyectivo y que $\mathrm{Ker}f = \mathrm{Mat}_{2\times 2}(7\mathbb{Z})$, luego, por el Primer Teorema de Isomofía, se cumple que

$$\mathrm{Mat}_{2\times 2}(\mathbb{Z}) \Big/ \mathrm{Mat}_{2\times 2}(7\mathbb{Z}) \approx \mathrm{Mat}_{2\times 2}(\mathbb{Z}/7\mathbb{Z}).$$

Para probar el Segundo Teorema de Isomorfía necesitamos un resultado análogo al que relacionaba subgrupos y subgrupos normales (Teorema I.5.27). En este caso, relación se establece entre subanillos e ideales está planteada como un ejercicio, ver Ejercicio II.2.21, y sirve para practicar con las caracterizaciones de subanillos e ideales (Proposiciones II.1.17 y II.2.2).

Teorema II.3.13 (Segundo Teorema de Isomorfía). Sea R un anillo, I un ideal de R y A un subanillo de R, entonces se cumple que

$$A \Big/ (A \cap I) \quad \approx \quad (A + I) \Big/ I.$$

Demostración. Consideramos el homomorfismo de inclusión $i : A \to A + I$ dado por $i(a) = a + 0_R = a$ y el homomorfismo de paso al cociente $p : A + I \to (A + I)/I$ dado por $p(a + x) = (a + x) + I$. Por el Ejercicio II.2.21, i y p son homomorfismos de anillos y por la Propiedad II.3.6, $f = p \circ i : A \to (A + I)/I$ es también un homomorfismo de anillos.
Observamos que f es **sobreyectivo** porque dado $b + I \in (A + I)/I$ existen $a \in A$ y $x \in I$ tales que $b + I = (a + x) + I = a + I = f(a)$.
Por otro lado, tenemos que $\mathrm{Ker}f = A \cap I$ porque $f(a) = 0_{(A+I)/I}$ si y solo si $a + I = 0_R + I$ si y solo si $a \in I$.
Finalmente, por el Primer Teorema de Isomorfía, concluimos que $(A + I)/I \approx A/(A \cap I)$. ■

Ejemplo II.3.14 (1) En el anillos de los enteros $(\mathbb{Z}, +, \cdot)$ consideramos el subanillo $A = 4\mathbb{Z}$ y el ideal $I = 6\mathbb{Z}$. Por el Segundo Teorema de Isomofía tenemos que

$$(4\mathbb{Z} + 6\mathbb{Z}) \Big/ 6\mathbb{Z} \approx 4\mathbb{Z}/(4\mathbb{Z} \cap 6\mathbb{Z}).$$

Por el Ejercicio I.2.19, sabemos que $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$ y que $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$, luego

$$(2\mathbb{Z}) \Big/ 6\mathbb{Z} \approx 4\mathbb{Z}/(12\mathbb{Z}).$$

(2) En $\mathbb{R}[x]$ consideramos el subanillo $A=\mathbb{Z}[x]$ y el ideal $I=\{P(x)\in\mathbb{R}[x] \,:\, P(0)=0\}=(x)$. Por el Segundo Teorema de Isomorfía tenemos que $(\mathbb{Z}[x]+(x))\Big/(x)\approx\mathbb{Z}[x]\Big/(\mathbb{Z}[x]\cap(x))$.

Para demostrar los dos primeros teoremas de isomorfía hemos realizado la prueba de forma directa sin usar los teoremas para grupos. Sin embargo, como veremos en este último caso, las pruebas anteriores pueden simplificarse si se emplean los resultados conocidos para grupos.

Teorema II.3.15 (Tercer Teorema de Isomorfía). Sea R un anillo e I,J ideales de R con $I\subseteq J$. Entonces J/I es un ideal de R/I y se tiene que

$$(R/I)\Big/(J/I) \quad\approx\quad R\Big/J.$$

Demostración. Consideramos $f:R/I\to R/J$ dada para todo $a\in R$ por $f(a+I)=a+J$, por la prueba del Teorema I.6.23 (Tercer Teorema de Isomorfía para grupos), sabemos que f está bien definida y es un homomorfismo sobreyectivo entre los grupos $(R/I,+)$ y $(R/J,+)$. Observamos que $f((a+I)(b+I))=f((ab)+I)=(ab)+J=(a+J)(b+J)=f(a+I)f(b+I)$, es decir, f es un homomorfismo de anillos. Por la prueba del Terecer I.6.23, sabemos también que $\mathrm{Ker} f=J/I$ y, por tanto, J/I es un ideal de R/I y, por el primer teorema de isomorfía, concluimos que $(R/I)/(J/I)\approx R/J$. ■

Ejemplos II.3.16 (1) Observamos que $7\mathbb{Z}$ y $28\mathbb{Z}$ son subanillos e ideales de $\mathbb{Z}$ con $28\mathbb{Z}\subseteq 7\mathbb{Z}$. Consideramos los anillos $(\mathbb{Z}/28\mathbb{Z},+,)$ y $(7\mathbb{Z}/28\mathbb{Z},+,\cdot)$ y por el Tercer teorema de Isomofía se tiene que

$$(\mathbb{Z}/28\mathbb{Z})\Big/(7\mathbb{Z}/28\mathbb{Z})\approx(\mathbb{Z}/7\mathbb{Z}).$$

(2) En $\mathbb{Z}[x]$ consideramos $I=(2)$ y $J=(2,x^2+x+1)$ y observamos que $(2)\subseteq(2,x^2+x+1)$ y consideramos los anillos $(\mathbb{Z}[x]/(2),+,\cdot)$ y $((2,x^2+x+1)/(2),+,\cdot)$, luego por Tercer teorema de Isomofía se tiene que

$$(\mathbb{Z}[x]/(2))\Big/((2,x^2+x+1)/(2))\approx(\mathbb{Z}[x]/(2,x^2+x+1)).$$

II.3.3 Teorema chino del resto

Gran parte de los resultados de teoría de anillos son generalizaciones a un anillo cualquiera de resultados que son ciertos en $(\mathbb{Z},+,\cdot)$. El teorema chino del resto en los enteros establece un isomorfismo entre los enteros módulo $N\in\mathbb{N}_{\geq 1}$ y el producto cartesiano de los enteros módulo $n_j\in\mathbb{N}_{\geq 1}$, donde $N=n_1n_2\cdots n_k$ con n_j dos a dos primos entre sí. Este isomorfismo puede extenderse para anillos arbitrarios. Recordamos que, por el Ejercicio II.1.24, se puede definir una estructura de anillo sobre el producto de un conjunto de anillos definiendo la suma y el producto componente a componente.

Teorema II.3.17 (Teorema chino del resto). Sea $(R,+,\cdot)$ un anillo, $n\in\mathbb{N}_{\geq 1}$ e $I_1,I_2,\ldots I_n\subseteq R$ ideales tales que se cumple que

$$(\star)\text{ para todo } j\in\{1,2,\ldots,n\}\qquad I_j+\bigcap_{\substack{k\neq j\\ k\in\{1,2,\ldots,n\}}} I_k=R,$$

entonces se tiene que

$$R/(I_1\cap I_2\cap\cdots\cap I_n)\qquad\approx\qquad R/I_1\times R/I_2\times\cdots\times R/I_n.$$

Demostración. Consideramos la aplicación de paso al cociente $f : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$ dada por

$$f(a) = (a+I_1, a+I_2, \ldots, a+I_n).$$

Tenemos que f es un homomorfismo de anillos por ser un homomorfismo de anillos en cada componente del producto $S := \prod_{j=1}^n R/I_j$. Observamos que:

$$f(a) = 0_S \quad \Leftrightarrow \quad a \in I_1, a \in I_2, \ldots, a \in I_n \quad \Leftrightarrow \quad a \in \cap_{j=1}^n I_j.$$

En consecuencia, se tiene que $\mathrm{Ker} f = \cap_{j=1}^n I_j$. Probaremos a continuación que f es sobreyectivo. Dados $a_1, a_2, \ldots, a_n \in R$ vamos a demostrar que existe $x \in R$ tal que para todo $j \in \{1,2,\ldots,n\}$ se cumple que $x + I_j = a_j + I_j$. Por la condición $(\star)$, para todo $j \in \{1,2,\ldots,n\}$ podemos escribir

$$a_j = c_j + d_j \quad \text{con} \quad c_j \in I_j \quad \text{y} \quad d_j \in \bigcap_{\substack{k \neq j \\ k \in \{1,2,\ldots,n\}}} I_k.$$

Tomamos $x = d_1 + d_2 + \cdots + d_n$ y comprobamos que para todo $j \in \{1,2,\ldots,n\}$ se satisface que $x + I_j = d_j + I_j = (a_j - c_j) + I_j = a_j + I_j$. De manera que $f(x) = (x+I_1, x+I_2, \ldots, x+I_n) = (a_1+I_1, a_2+I_2, \ldots, a_n+I_n)$, es decir, f es sobreyectivo. Finalmente, por el primer teorema de isomorfía se concluye que

$$R/\bigcap_{j=1}^n I_j = R/(\mathrm{Ker} f) \approx \mathrm{Im} f = \prod_{j=1}^n R/I_j.$$

■

Ejemplos II.3.18 Veamos como se interpretan las condición $(\star)$ de este teorema en $(\mathbb{Z}, +, \cdot)$. Por el Ejercicio II.2.20, sabemos que I es un ideal de $\mathbb{Z}$ si y solo si es de la forma $I = m\mathbb{Z}$ con $m \in \mathbb{N}$. Por tanto, la condición $(\star)$ se puede reescribir como: tenemos $m_1, m_2 \ldots, m_n \in \mathbb{N}$ tales que

$$(\star) \text{ para todo } j \in \{1,2,\ldots,n\} \qquad m_j\mathbb{Z} + \bigcap_{k \neq j \ k \in \{1,2,\ldots,n\}} m_k\mathbb{Z} = \mathbb{Z}.$$

Nuestro objetivo es probar que

$$(\star) \quad \Leftrightarrow \quad \text{m.c.d.}\,(m_k, m_j) = 1 \qquad \forall k, j \in \{1,\ldots,n\}.$$

Recordamos que por el Ejercicio I.2.19 se tiene que

$$\bigcap_{k \neq j \ k \in \{1,2,\ldots,n\}} m_k\mathbb{Z} = \text{m.c.m.}\,(\{m_k \ : \ k \neq j, \ k \in \{1,2,\ldots,n\}\})$$

y por ese mismo ejercicio sabemos que

$$m_j\mathbb{Z} + \bigcap_{k \neq j \ k \in \{1,2,\ldots,n\}} m_k\mathbb{Z} = \text{m.c.d.}\,(m_j, \text{m.c.m.}\,(\{m_k \ : \ k \neq j, \ k \in \{1,2,\ldots,n\}\})).$$

Por la Identidad de Bezout (Corolario A.2.10 y ObservaciónA.2.11), se tiene que

$$(\star) \quad \Leftrightarrow \quad \text{m.c.d.}\,(m_j, \text{m.c.m.}\,(\{m_k \ : \ k \neq j, \ k \in \{1,2,\ldots,n\}\})) = 1.$$

Finalmente, como en el Corolario A.2.13.(VIII) podemos probar la siguiente igualdad

$$\text{m.c.d.}\,(a, \text{m.c.m.}\,(b_1, b_2, \ldots, b_r)) = \text{m.c.m.}\,(\text{m.c.d.}\,(a, b_1), \text{m.c.d.}\,(a, b_2), \ldots, \text{m.c.d.}\,(a, b_r))$$

y deducir que para todo $j \in \{1,\dots,n\}$ se tiene que

$$\begin{array}{r} \text{m.c.d.}\,(m_k,m_j)=1, \\ \forall k \in \{1,\dots,n\} \end{array} \quad \Leftrightarrow \quad \text{m.c.d.}\,(m_j, \text{m.c.m.}\,(\{m_k \,:\, k\neq j,\, k\in\{1,2,\dots,n\}\}))=1.$$

Por tanto, el Teorema Chino del Resto se puede aplicar a cualquier conjunto de números naturales que sean **primos entre sí.** En otras palabras, si para todos $k,j \in \{1,\dots,n\}$ tenemos que $\text{m.c.d.}\,(m_k,m_j)=1$, entonces se cumple que

$$\mathbb{Z}/\text{m.c.m.}\,(m_1,\dots,m_n)\mathbb{Z} \overset{\text{E. II.2.20}}{=} \mathbb{Z}\Big/(m_1\mathbb{Z}\cap m_2\mathbb{Z}\cap\cdots\cap m_n\mathbb{Z}) \approx \mathbb{Z}/m_1\mathbb{Z}\times\mathbb{Z}/m_2\mathbb{Z}\times\cdots\times\mathbb{Z}/m_1\mathbb{Z}$$

Por ejemplo,como $\text{m.c.d.}\,(3,5)=1$ o como $\text{m.c.d.}\,(2,7)=1$, $\text{m.c.d.}\,(7,9)=1$ y $\text{m.c.d.}\,(2,9)=1$ se tiene que

$$\mathbb{Z}/15\mathbb{Z} \approx \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z} \qquad\qquad \mathbb{Z}/126\mathbb{Z} \approx \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}.$$

Obtener una representación de la intersección de un conjunto de ideales puede ser bastante complicado y, por este motivo, buscamos una representación más práctica de la condición $(\star)$ y de la intersección de los ideales $\bigcap_{j=1}^{n} I_j$ que aparece en el anillo cociente. La condición $(\star)$ se puede simplificar gracias al Ejercicio II.2.26. Por otra parte, la intersección de ideales se puede reescribir para en anillos conmutativos y unitarios empleando el **producto de ideales**, ver Ejercicio II.2.22 para la definición. En general, no podemos afirmar que $IJ = I\cap J$, pero si R es un anillo conmutativo y unitario y se cumplen ciertas condiciones adicionales sí se satisface la igualdad, ver Ejercicio II.2.24.

Teorema II.3.19 (Teorema chino del resto en anillos conmutativos y unitarios). Sea $(R,+,\cdot)$ un anillo conmutativo y unitario e $I_1,I_2,\dots,I_n$ ideales de R tales que $I_k+I_j=R$ si $k\neq j$. Entonces:

(I) para todo $j\in\{1,2,\dots,n\}$ se tiene que $I_j + \displaystyle\bigcap_{k\in\{1,2,\dots,n\},\ k\neq j} I_k = R$,

(II) se tiene que $I_1I_2\cdots I_n = I_1\cap I_2\cap\cdots\cap I_n$.

(III) se cumple que

$$R/(I_1I_2\cdots I_n) \qquad \approx \qquad R/I_1\times R/I_2\times\cdots\times R/I_n.$$

Observación II.3.20 Con esta reescritura se ve, de forma directa por la Identidad de Bezout, que la condición $I_k+I_j=R$ si $k\neq j$ se traduce en $\mathbb{Z}$ como $\text{m.c.d.}\,(m_k,m_j)=1$ si $I_k=m_k\mathbb{Z}$ y $I_j=m_j\mathbb{Z}$ como habíamos probado en el Ejemplo II.3.18.

Ejercicio II.3.21 Probar las Propiedades II.3.3 de los homomorfismos de anillos.

Ejercicio II.3.22 Probar la Propiedades II.3.6 sobre la composición de homomorfismos.

Ejercicio II.3.23 ¿Existen dos anillos $(R,+,\cdot)$ y $(S,+,\cdot)$ y $f:(R,+)\to(S,+)$ un homomorfismo entre los grupos aditivos que no sea homomorfismo de anillos, es decir, f satisface (HA.I) pero no satisface (HA.II)?

Ejercicio II.3.24 ¿Se puede construir un homomorfismo entre dos anillos unitarios que sea homomorfismo de anillos pero que no sea homomorfismo de anillos unitarios?

Ejercicio II.3.25 Determinar si las siguientes aplicaciones son o no homomorfismos de anillos:
(I) $f:\mathbb{Z}/5\mathbb{Z}\to\mathbb{Z}/10\mathbb{Z}$ dada por $f(x)=5x$.
(II) $f:\mathbb{Z}/5\mathbb{Z}\to\mathbb{Z}/30\mathbb{Z}$ dada por $f(x)=6x$.
(III) $f:\mathbb{Z}/10\mathbb{Z}\to\mathbb{Z}/10\mathbb{Z}$ dada por $f(x)=2x$.
(IV) $f:\mathbb{Z}/4\mathbb{Z}\to\mathbb{Z}/12\mathbb{Z}$ dada por $f(x)=3x$.
¿Son homomorfismos de anillos unitarios?

Ejercicio II.3.26 Demostrar que todo homomorfismo de anillos $f:\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ es de la forma $f(x)=ax$ para algún $a\in\mathbb{Z}/n\mathbb{Z}$ idempotente. Si f es homomorfismo de anillos unitarios, ¿Qué posibilidades hay para f?

Ejercicio II.3.27 Probar que si $f:\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ es un homomorfismo de anillos entonces $f(1)=a$ para algún $a\in\mathbb{Z}/m\mathbb{Z}$ idempotente. Demostrar que esta condición es necesaria pero no suficiente para que f sea homomorfismo.

Ejercicio II.3.28 Si $f:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$ es un homomorfismo de anillos unitarios, ¿qué valores puede tomar $f(1,0)$?

Ejercicio II.3.29 Determinar todos los homomorfismos de anillos unitarios $f:H\to G$ en los siguientes casos:
(I) $G=H=\mathbb{Z}$,
(II) $G=H=\mathbb{Z}\times\mathbb{Z}$,
(III) $G=\mathbb{Z}\times\mathbb{Z}$ y $H=\mathbb{Z}$,
(IV) $G=H=\mathbb{Q}$.

Ejercicio II.3.30 Determinar un sistema completo de representantes de las clases del anillo $R=\mathbb{Z}[x]/(x^2+1)$ y comprobar que R es isomorfo a $\mathbb{Z}[i]$.

Ejercicio II.3.31 Probar que los anillos:

$$\left\{\begin{pmatrix} a & 2b \\ b & a\end{pmatrix} : a,b\in\mathbb{Z}\right\} \qquad y \qquad \mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2} \ : \ a,b\in\mathbb{Z}\}$$

son isomorfos.

Ejercicio II.3.32 Dado $(R,+,\cdot)$ un anillo unitario, consideramos el homomorfismo característico:

$$\begin{array}{rcl} \kappa:\mathbb{Z} & \to & R \\ m & \to & \kappa(m) \quad = m\cdot 1_R = 1_R+\cdots(m \text{ veces})\cdots+1_R \end{array}$$

Se pide:
(I) Probar que κ es el único homomorfismo de anillos unitarios de $\mathbb{Z}$ en R.
(II) Probar que Im κ es el menor subanillo unitario contenido en R.
(III) Probar que existe $n\in\mathbb{N}$ tal que Im $\kappa\approx\mathbb{Z}/n\mathbb{Z}$ y deducir que $\text{car}(R)=n$.
Como consecuencia, de forma alternativa y equivalente, podemos definir la característica del anillo R como el único número $n\in\mathbb{N}$ tal que R contenga un subanillo isomorfo al anillo cociente $\mathbb{Z}/n\mathbb{Z}$ (Observad que $\mathbb{Z}/0\mathbb{Z}=\mathbb{Z}/\{0\}\approx\mathbb{Z}$). En este sentido, decimos que R tiene característica $n\in\mathbb{N}$ porque n caracteriza la imagen canónica de $\mathbb{Z}$ en R.

Ejercicio II.3.33 Dados R y S anillos conmutativos unitarios y $f : R \to S$ un homomorfismo de anillos sobreyectivo. Probar que $\mathrm{car}(S) \mid \mathrm{car}(R)$. Deducir que dos anillos isomorfos tienen la misma característica.

Ejercicio II.3.34 Estableciendo un isomorfismo adecuado, determinar la característica del anillo $\mathbb{Z}[i]/(2+i)$. (ver Ejemplo II.2.14)

Ejercicio II.3.35 Probar, haciendo uso del teorema chino del resto, que
(I) $\mathbb{Z}/30 \approx \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \approx \mathbb{Z}/2 \times \mathbb{Z}/15\mathbb{Z} \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.
(II) $\mathbb{Q}[x]/(x^2-1) \approx \mathbb{Q}[x]/(x+1) \times \mathbb{Q}[x]/(x-1)$.

Ejercicio II.3.36 ¿Es cierto que $\mathbb{R}[x,y]/(xy) \approx \mathbb{R}[x,y]/(x) \times \mathbb{R}[x,y]/(y)$?

II.4 Dominios y cuerpos

II.4.1 Nociones básicas

Se podría afirmar que la noción de de anillo se establece para intentar extrapolar las propiedades algebraicas de los de los enteros $(\mathbb{Z},+,\cdot)$ a un contexto abstracto. Sin embargo, la noción de anillo no es la generalización más fiel de los enteros. A parte de las dos propiedades obvias, conmutatividad y existencia de elemento neutro para el producto, hay otro rasgo fundamental que posee el anillo de los enteros y que no poseen los anillos conmutativos y unitarios en general: se verifica **la ley de cancelación**. En esta sección introducimos un tipo particular de anillos que tienen estas tres propiedades: los dominios de integridad.

Definición II.4.1 Sea $(D,+,\cdot)$ un anillo, decimos que D es un **dominio de integridad** o simplemente un **dominio** si se tiene que

(D.I) D es un anillo conmutativo.

(D.II) D es un anillo unitario.

(D.III) el único divisor de cero en D es 0_D.

Estrechamente ligada a la noción de dominio tenemos la noción de cuerpo.

Definición II.4.2 Sea $(F,+,\cdot)$ un anillo, decimos que F es un **cuerpo** si se tiene que

(F.I) F es un anillo conmutativo.

(F.II) F es un anillo unitario.

(F.III) $U(F) = F\backslash\{0_F\}$.

(En otras palabras, F es cuerpo si y solo si $(F,+,\cdot)$ es un anillo y $(F\backslash\{0_F\},\cdot)$ es un grupo conmutativo).

Ejemplos II.4.3 (1) $(\mathbb{Z},+,\cdot)$ y $(\mathbb{Q},+,\cdot)$ son dominios, pero $\mathbb{Q}$ es cuerpo y $\mathbb{Z}$ no.

(2) Los anillos (a) $(\mathrm{Mat}_{3\times 3}(\mathbb{Z}),+,\cdot)$, (b) $(\mathbb{Z}/12\mathbb{Z},+,\cdot)$, (c) $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$ y (d) $(5\mathbb{Z},+,\cdot)$ no son dominios.

Teorema II.4.4 Todo cuerpo es un dominio de integridad.

Demostración. Sea $(F,+,\cdot)$ un cuerpo como F satisface (F.I) y (F.II) satisface (D.I) y (D.II) y, por tanto, sólo es necesario comprobar que se cumple la propiedad (D.III). Por (F.II), existe $1_F \in F$ y $1_F \in U(F)$, por (F.III), $F\backslash\{0_F\} = U(F)$, luego $1_F \neq 0_F$. Por lo que existe $a \in F$ con $a \neq 0_F$ y tenemos que $0_F a = 0_F$. Por esta razón, 0_F es divisor del cero.
Veamos ahora que 0_F es el único divisor de cero. Dados $a,b \in F$ con $a \cdot b = 0_F$, si $a \neq 0_F$ entonces, por (F.III), $a \in U(F)$ y observamos que:

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

Análogamente, vemos que si $b \neq 0_F$, entonces $a = 0_F$. Por consiguiente, F verifica (D.III) y concluimos que F es un dominio. ■

Observación II.4.5 Se cumple que

$$\{\text{Cuerpos}\} \subseteq \{\text{Dominios de integridad}\} \subseteq \{\text{Anillos conmutativos y unitarios}\}$$

y el contenido es estricto en ambos casos.

De ahora en adelante, vamos a centrar nuestro estudio en analizar cómo se pueden extender las propiedades del dominio de enteros a cualquier dominio. En particular, aunque en un dominio pueda haber elementos que no tienen inversos para el producto la ley de cancelación sigue siendo válida gracias a la conjunción de la propiedad distributiva y a (D.III).

Proposición II.4.6 — Ley de cancelación. Sean D un dominio y $a,b,c \in D$ con $a \neq 0_D$. Se cumple que

$$\text{si} \quad ab = ac, \quad \text{entonces} \quad b = c.$$

Demostración. Dados $a,b,c \in D$ con $a \neq 0_D$, tales que $ab = ac$, sumando a ambos lados el inverso aditivo de ac, observamos que $ab - ac = 0_D$ y, por la propiedad distributiva, vemos que $a(b-c) = 0_D$. Como D es un dominio y $a \neq 0_D$, por la propiedad (D.III), deducimos que $b - c = 0_D$ y, sumando a ambos lados c, concluimos que $b = c$. ■

Veamos ahora que que con alguna propiedad adicional un dominio es un cuerpo.

Teorema II.4.7 Todo dominio de integridad finito es un cuerpo.

Demostración. Sea $(D,+,\cdot)$ un dominio como D satisface (D.I) y (D.II) satisface (F.I) y (F.II) y, por tanto, sólo es necesario comprobar que se cumple la propiedad (F.III).
Veamos que $U(D) = D\backslash\{0_D\}$ por doble contenido.
$(\subseteq)$ Tomamos $a \in U(D)$, si a fuera igual a 0_D, por (D.III) como 0_D es divisor del cero entonces existe $b \in D$, $b \neq 0_D$ tal que $ab = 0_D b = 0_D$. Observamos que

$$b = 1_D b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0_D = 0_D,$$

lo que es absurdo porque $b \neq 0_D$. En consecuencia, $a \neq 0_D$ y $U(D) \subseteq D\backslash\{0_D\}$.
$(\supseteq)$ Tomamos $a \in D$ con $a \neq 0_D$, consideramos el subconjunto de D, $A := \{a^k : k \in \mathbb{N}\}$. Como D es finito, A es finito, por lo cual, existen $m,\ell \in \mathbb{N}$ tales que $a^m = a^\ell$ con $m > \ell$. Por (D.III), como $a \neq 0_D$, a no es divisor del cero y se tiene $a^\ell \neq 0_D$. Escribimos $m = \ell + k$ con $k \in \mathbb{N}_{\geq 1}$ y observamos que $a^\ell a^k = a^m = a^\ell = a^\ell 1_D$. Por la Ley de cancelación, deducimos que $a^k = 1_D$, luego $a^{k-1}a = 1_D$, es decir, a^{k-1} es el inverso de a para el producto y $a \in U(D)$. Concluimos que $D\backslash\{0_D\} \subseteq U(D)$, por lo que se satisface (F.III). ■

Ejemplo II.4.8 Sea $n \in \mathbb{N}_{\geq 1}$. Vamos a probar que son equivalentes:

(I) n es primo,

(II) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ es un dominio,

(III) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ es un cuerpo.

Demostración. Sabemos que el anillo $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ es conmutativo y unitario para todo $n \in \mathbb{N}_{\geq 1}$ (ver Ejercicio I.1.6). [**].
Por tanto, sólo hay que ver que ocurre con las propiedades (D.III) y (F.III).

$\boxed{\text{(I)} \Rightarrow \text{(II)}}$ Veamos que 0 es divisor de cero. Como n es primo $n > 1$, luego $1 \neq 0$ y $1 \cdot 0 = 0$ en $\mathbb{Z}/n\mathbb{Z}$. Por ello, 0 es divisor de cero.

Veamos que 0 es el único divisor de cero.
Dados $a, b \in \mathbb{Z}/n\mathbb{Z}$ con $ab = 0$ en $\mathbb{Z}/n\mathbb{Z}$, tenemos que $n \mid ab$. Por lo tanto, como n es primo $n|a$ o $n|b$, es decir, $a = 0$ ó $b = 0$. En otras palabras, 0 es el único divisor de cero, se satisface (D.III) y $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ es un dominio.

$\boxed{\text{(II)} \Rightarrow \text{(III)}}$ Directo empleando el Teorema II.4.7 porque $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ es finito.

$\boxed{\text{(III)} \Rightarrow \text{(I)}}$ Veamos que $\neg\text{(I)} \Rightarrow \neg\text{(III)}$ y supongamos que n no es primo.
Si $n = 1$, entonces $\mathbb{Z}/1\mathbb{Z} = \{0\}$ y 0 no es un divisor del cero, por lo que $(\mathbb{Z}/1\mathbb{Z}, +, \cdot)$ no es un dominio y, por el Teorema II.4.4, $(\mathbb{Z}/1\mathbb{Z}, +, \cdot)$ no es un cuerpo.
Si $n > 1$ y n no es primo, entonces, por la Proposición A.2.20, existen $r, s \in \{2, 3, \ldots, n-1\}$ con $n = rs$. Por este motivo, se tiene que $rs = 0$ en $\mathbb{Z}/n\mathbb{Z}$, pero $r \neq 0$ y $s \neq 0$, es decir, r y s son divisores de cero no nulos. Debido a lo cual, 0 no es el único divisor de cero por lo que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ no es un dominio y, por el Teorema II.4.4, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ no es un cuerpo. ■

De esta forma, $(\mathbb{Z}/37\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}/73\mathbb{Z}, +, \cdot)$ son dominios y cuerpos, pero los anillos $(\mathbb{Z}/6\mathbb{Z}, +, \cdot)$ y $(\mathbb{Z}/21\mathbb{Z}, +, \cdot)$ no son ni dominios ni cuerpos.

Este ejemplo ilustra un fenómeno más general que se cumple en cualquier dominio relacionado con la noción de característica. Realizaremos la demostración de forma directa empleando el Teorema II.2.16, aunque también es posible realizar la demostración mediante el empleando el homomorfismo característico $\kappa : \mathbb{Z} \to D$, ver Ejercicio II.3.32

Corolario II.4.9 La característica de un dominio es o bien 0 o bien $p \in \mathbb{N}_{\geq 1}$ con p primo.

Demostración. Por el Teorema II.2.16, como los dominios son anillos unitarios (D.II), basta estudiar el orden aditivo del 1_D.
Si $O(1_D) = \infty$, entonces $\text{car}(D) = 0$ y hemos terminado.
Si $O(1_D) < \infty$, sabemos que $\text{car}(D) = O(1_D)$. Veamos que $n = O(1_D)$ es primo.
Veamos que $n \neq 1$. Razonando por reducción al absurdo, si $1_D = 0_D$, tendríamos que $d = d \cdot 1_D = d \cdot 0_D = 0_D$ para todo $d \in D$. Por consiguiente, $D = \{0_D\}$ pero en este anillo 0_D no es divisor de cero contradiciendo (D.III).
Por tanto, $n > 1$. Razonando de nuevo por reducción al absurdo, suponemos que n no es primo, es decir, existen $1 < s, t < n$ con $n = st$. Por la Propiedad II.1.14.(VI), se tiene que

$$0 = n1_D = (st)1_D = (s1_D)(t1_D).$$

Por (D.III), tenemos que o $s1_D = 0$ o $t1_D = 0$, lo que contradice que n es el menor natural que satisface que $n1_D = 0$. En consecuencia, $n = O(1_D) = \text{car}(D)$ debe ser primo. ■

[**]Se podría probar también que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ es conmutativo y unitario para todo $n \in \mathbb{N}_{\geq 1}$ porque es isomorfo al anillo cociente módulo $n\mathbb{Z}$ de $(\mathbb{Z}, +, \cdot)$, que es un anillo conmutativo y unitario

II.4.2 Ideales primos e ideales maximales

Definición II.4.10 Sean $(R,+,\cdot)$ un anillo conmutativo e I un ideal de R. Decimos que I es un **ideal primo** si se cumplen

(P.I) $I \neq R$,

(P.II) para todos $a,b \in R$ tales que $ab \in I$ se tiene que $a \in I$ o $b \in I$.

Definición II.4.11 Sean $(R,+,\cdot)$ un anillo conmutativo e I un ideal de R. Decimos que I es un **ideal maximal** si se cumplen

(M.I) $I \neq R$,

(M.II) para todo ideal J de R con $I \subseteq J \subseteq R$ se tiene que $I = J$ o $J = R$.

Ejemplos II.4.12 (1) En $\mathbb{Z}$ todo ideal de la forma $(p) = p\mathbb{Z}$, con $p \in \mathbb{N}_{\geq 1}$ primo, es maximal y primo.
Veamos que $p\mathbb{Z}$ es un **ideal primo**. Si p es primo, entonces $p > 1$ y, así, $1 \notin p\mathbb{Z}$, luego $p\mathbb{Z} \subsetneq \mathbb{Z}$, es decir, se cumple (P.I). Por otro lado, si $ab \in p\mathbb{Z}$, entonces $p \mid ab$ y, por ser p primo, o $p \mid a$ o $p \mid b$, luego o $a \in p\mathbb{Z}$ o $b \in p\mathbb{Z}$, es decir, se cumple (P.II).
Veamos que $p\mathbb{Z}$ es un **ideal maximal**. Hemos visto que se cumple (M.I), si $p\mathbb{Z} \subseteq J \subseteq \mathbb{Z}$, por la forma de los ideales de $\mathbb{Z}$, ver Ejercicio II.2.20, tenemos que $J = m\mathbb{Z}$ para algún $m \in \mathbb{N}_{\geq 1}$, como $p \in p\mathbb{Z} \subseteq J = m\mathbb{Z}$, tenemos que $m \mid p$ y, como p es primo, por la ProposiciónA.2.20, tenemos que $m = \pm 1$ o $m = \pm p$, es decir, o $J = m\mathbb{Z} = \mathbb{Z}$ o $J = m\mathbb{Z} = p\mathbb{Z}$, luego se cumple (M.II).

(2) El ideal de $\mathbb{Z}[x]$ generado por 2 y x (ver Observación II.2.9), es decir, el ideal

$$(2,x) = (\{2,x\}) = \{P(x)\cdot 2 + Q(x)\cdot x \ : \ P(x),Q(x) \in \mathbb{Z}[x]\}$$

es un ideal maximal de $\mathbb{Z}[x]$. Se trata de un ejercicio comprobar que $(2,x)$ es el ideal de los polinomios cuyo término independiente es par, es decir,

$$(2,x) = \{P(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x] \ : \ a_0 \in 2\mathbb{Z}\},$$

luego $1 \notin (2,x)$ y $(2,x) \subsetneq \mathbb{Z}[x]$. Se considera J un ideal con $(2,x) \subsetneq J \subseteq \mathbb{Z}[x]$. Como $(2,x) \subsetneq J$, tenemos que existe $Q \in J$ con $Q \notin (2,x)$, luego si $Q(x) = \sum_{j=0}^{m} b_j x^j$, entonces su término independiente b_0 es impar, luego $b_0 = 2k+1$ con $k \in \mathbb{Z}$. Observamos que podemos escribir

$$1 = \underbrace{Q(x)}_{\in J} \underbrace{- \sum_{j=1}^{m} b_j x^j - 2k}_{\in (2,x) \subseteq J} \in J.$$

Por consiguiente, se cumple que $1 \in J$ y que $J = \mathbb{Z}[x]$. (ver Ejercicio II.2.25)

(3) El ideal $(x) = \{Q(x)\cdot x : Q(x) \in \mathbb{Z}[x]\}$ es un ideal primo de $\mathbb{Z}[x]$ que no es maximal. Veamos que (x) es **primo**. Vemos que $1 \notin (x)$, luego $(x) \neq \mathbb{Z}[x]$.
Podemos comprobar que $(x) = \{P(x) \in \mathbb{Z}[x] \ : \ P(0) = 0\}$, es decir, que (x) coincide con el ideal de los polinomios que se anulan en 0 (ver Corolorio II.6.16). Razonando por contradicción, si $P_1 \cdot P_2 \in (x)$ y $P_1 \notin (x)$ y $P_2 \notin (x)$ tenemos que $P_1(0)P_2(0) = (P_1P_2)(0) = 0$, que $P_1(0) \neq 0$ y que $P_2(0) \neq 0$, lo que es imposible porque $\mathbb{Z}$ es un dominio. Por tanto, tenemos (x) cumple (P.I) y (P.II) y es primo. Sin embargo, (x) **no es maximal** porque

$$(x) \overset{2 \notin (x)}{\subsetneq} (2,x) \overset{\text{apartado anterior}}{\subsetneq} \mathbb{Z}[x].$$

Proposición II.4.13 Sea $(R,+,\cdot)$ un anillo conmutativo y unitario. Todo ideal maximal es un ideal primo.

Demostración. Sea I un ideal maximal, como satisface (M.I) satisface (P.I). Veamos que se satisface (P.II).
Dados $a,b \in R$ con $ab \in I$. Si $a \notin I$, entonces I está estrictamente contenido en el ideal $(I \cup (a))$, donde $(a) = \{ra : r \in R\}$ (Observación II.2.9) y, como I es maximal, por (M.II) tenemos que $R = (I \cup (a))$. Por la Proposición II.2.11, se tiene que $(I \cup (a)) = I + (a)$, luego $R = I + (a)$. Como R es unitario $1_R \in R = I + (a)$, luego existen $x \in I$ y $r \in R$ tales que $1_R = x + ra$. Multiplicando por b a ambos lados y, empleando la propiedad conmutativa, vemos que

$$b = b1_R = b(x + ra) = bx + rab.$$

Como $x \in I$, $bx \in I$ y como $ab \in I$, $rab \in I$ de forma que $b = bx + rab \in I$. Análogamente, si $b \notin I$ vemos que $a \in I$. En conclusión, I verifica (P.II). ■

Observación II.4.14 Si el anillo R no es unitario o no es conmutativo la proposición anterior es en general falsa. Por ejemplo, $9\mathbb{Z}$ es un ideal maximal del anillo $(3\mathbb{Z},+,\cdot)$ pero no es primo porque $3 \cdot 3 = 9 \in 9\mathbb{Z}$ pero $3 \notin 9\mathbb{Z}$.

Teorema II.4.15 Sean $(R,+,\cdot)$ un anillo conmutativo y unitario e I un ideal de R. Entonces

(I) R/I es dominio $\Leftrightarrow$ I es un ideal primo.

(II) R/I es cuerpo $\Leftrightarrow$ I es un ideal maximal.

Demostración. Como $(R,+,\cdot)$ es un un anillo conmutativo y unitario $(R/I,+,\cdot)$ es también un anillo conmutativo y unitario para todo ideal I de R. En otras palabras, sólo hace falta ver que ocurre con las propiedades (D.III) y (F.III) en cada caso.

(I) $\boxed{\Rightarrow}$ Supongamos que R/I es un dominio. Por (D.III), $0_{R/I} = 0_R + I$ es divisor del cero, es decir, existe $c + I \in R/I$ con $c + I \neq 0_{R/I}$ tal que $(c+I)(0_R+I) = 0_R + I$. Como $c + I \neq 0_R + I$, tenemos que $c \notin I$ y, por tanto, $I \neq R$ y se satisface (P.I).
Dados $a,b \in R$ con $ab \in I$, observamos que $(a+I)(b+I) = (ab) + I = I = 0_{R/I}$. Por (D.III), o $a + I = 0_{R/I} = I$ o $b + I = 0_{R/I} = I$, es decir, o $a \in I$ o $b \in I$. Por consiguiente, I verifica (P.II).
$\boxed{\Leftarrow}$ Supongamos que I es un ideal primo. Por (P.I), existe $c \in R$ con $c \notin I$, luego $c + I \neq 0_{R/I}$ y se cumple que $(c+I)(0_R+I) = 0_{R/I}$, es decir, $0_{R/I}$ es divisor del cero.
Veamos ahora que es el único divisor del cero. Dados $a,b \in R$ con $(a+I)(b+I) = 0_{R/I}$. Tenemos que $(ab) + I = (a+I)(b+I) = 0_{R/I} = I$, luego $ab \in I$. Por (P.II), o $a \in I$ o $b \in I$, es decir, o $a + I = I$ o $b + I = I$, por lo cual se satisface (D.III).

(II) $\boxed{\Rightarrow}$ Supongamos que R/I es un cuerpo. Por el Teorema II.4.4, R/I es un dominio y, por el apartado (I), I es primo, luego I satisface (P.I) y, por tanto, I satisface (M.I).
Dado $J \subseteq R$ un ideal con I estrictamente contenido en J tenemos que existe $b \in J$ tal que $b \notin I$. Por este motivo, $b + I \neq I = 0_{R/I}$ y, por (F.III), $b + I \in U(R/I)$. En otras palabras, existe $c \in R$ tal que $(c+I)(b+I) = 1_{R/I} = 1_R + I$ y deducimos que $(bc) + I = 1_R + I$. Así pues, $1_R - (bc) \in I \subseteq J$ y, como $b \in J$, $bc \in J$ concluyendo que $1_R = (1_R - (bc)) + bc \in J$. Por lo tanto, se cumple que $J = R$ y concluimos que se verifica (M.II).

(⇐) Supongamos que I es un ideal maximal y probaremos que $U(R/I) = (R/I)\backslash\{0\}$ por doble contenido.
(⊆) Razonando por contradicción, dado $x+I \in U(R/I)$, si $x+I = 0_{R/I}$, entonces se cumple que

$$1_R + I = 1_{R/I} = (x+I)(x+I)^{-1} = (0_R+I)(x+I)^{-1} = I.$$

En ese caso, $1_R \in I$ y tendríamos que $I = R$ contradiciendo (M.I). En consecuencia, se verifica que $U(R/I) \subseteq (R/I)\backslash\{0_{R/I}\}$.
(⊇) Recíprocamente, dado $a+I \in (R/I)\backslash\{0_{R/I}\}$, tenemos que $a+I \neq I$, es decir, $a \notin I$. Por (M.II), $R = I+(a)$ y deducimos que existen $x \in I$ y $r \in R$ tales que $1_R = x+ra$. Por consiguiente, se cumple que

$$1_R + I = (x+I)+(ra+I) = I+(ra+I) = (ra)+I = (r+I)(a+I).$$

En otros términos $r+I$ es el inverso de $a+I$, entonces $(R/I)\backslash\{0_{R/I}\} \subseteq U(R/I)$ y concluimos que R/I verifica (F.III). ■

Ejemplos II.4.16 (1) Por lo probado en el Ejemplo II.4.12, tenemos que $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ con $p \in \mathbb{N}_{\geq 1}$ primo, es un cuerpo y un dominio (como ya habíamos visto en el Ejemplo II.4.8). Por otra parte $\mathbb{Z}[x]/(2,x)$ es un cuerpo y $\mathbb{Z}[x]/(x)$ es un dominio que no es un cuerpo.

(2) Probar que el anillo cociente $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2+1)$ no es un dominio.

Por el Teorema II.4.15, $(\mathbb{Z}/2\mathbb{Z})[x]/I$ es un dominio si y solamente si I es un ideal primo. Por tanto, basta ver que $\left(x^2+1\right) = \{Q(x)(x^2+1) : Q(x) \in (\mathbb{Z}/2\mathbb{Z})[x]\}$ no es primo. Observamos que en $(\mathbb{Z}/2\mathbb{Z})[x]$ se tiene que

$$(x+1)^2 = x^2+2x+1 = x^2+1,$$

es decir, $(x+1)(x+1) \in I = \left(x^2+1\right)$. Sin embargo, $(x+1) \notin \left(x^2+1\right)$, porque si $(x+1) = Q(x)(x^2+1)$ con $Q(x) = a_0 + a_1x + \cdots + a_nx^n$ y $a_i \in \mathbb{Z}/2\mathbb{Z}$ para todo $i \in \{0,1,2,\ldots,n\}$ se tendría, igualando coeficientes, que

$$a_0 = 1, \quad a_1 = 1, \quad a_k + a_{k-2} = 0 \quad \text{si} \quad k \in \{2,\ldots,n\} \quad \text{y} \quad a_n = a_{n-1} = 0,$$

que es un sistema que no tiene solución en $\mathbb{Z}/2\mathbb{Z}$. En consecuencia, $\left(x^2+1\right)$ no es un ideal primo y $(\mathbb{Z}/2\mathbb{Z})[x]/\left(x^2+1\right)$ no es un dominio.

II.4.3 Cuerpo de fracciones de un dominio

Hemos visto que todo cuerpo es un dominio y que todo dominio finito es un cuerpo. En este apartado veremos que aunque, en general, los dominios infinitos no son cuerpos podemos construir a partir de ellos un cuerpo que los contiene. El ejemplo clásico del procedimiento que vamos a describir de un modo abstracto es la construcción del cuerpo de los racionales empleado el dominio de los enteros.

Teorema II.4.17 Sea D un dominio. Entonces existe un cuerpo F con las siguientes propiedades:

(I) F contiene a un subanillo $\tilde{D}$ isomorfo a D.

(II) Si L es un cuerpo tal que $\tilde{D} \subseteq L \subseteq F$, entonces $L = F$.

Demostración. **Existencia:** Por (D.III), como 0_D es divisor del cero en D tenemos que $S := D\backslash\{0_D\} \neq \emptyset$ y consideramos $D \times S = \{(d,s) : d \in D \text{ y } s \in S\}$. En este conjunto definimos la siguiente relación

$$(d_1,s_1)\,R\,(d_2,s_2) \quad \Leftrightarrow \quad d_1s_2 = d_2s_1.$$

Se comprueba R es una relación de equivalencia (reflexiva, simétrica y transitiva). Definimos $F := (D\times S)/R$ y representamos por d/s **a la clase de** $[(d,s)]_R$. Definimos las operaciones:

$$\begin{array}{rcl} + : F\times F & \longrightarrow & F \\ \left(\frac{d_1}{s_1},\frac{d_2}{s_2}\right) & \longrightarrow & \frac{d_1s_2+d_2s_1}{s_1s_2} \end{array} \qquad \begin{array}{rcl} \cdot : F\times F & \longrightarrow & F \\ \left(\frac{d_1}{s_1},\frac{d_2}{s_2}\right) & \longrightarrow & \frac{d_1d_2}{s_1s_2} \end{array}$$

Vemos que estas operaciones están **bien definidas**. Sean $d_1/s_1 = \tilde{d_1}/\tilde{s_1}$ y $d_2/s_2 = \tilde{d_2}/\tilde{s_2}$, es decir, $d_1\tilde{s_1} = \tilde{d_1}s_1$ y $d_2\tilde{s_2} = \tilde{d_2}s_2$. Tenemos que

$$\begin{aligned} (d_1s_2+d_2s_1)(\tilde{s_1}\tilde{s_2}) &= d_1\tilde{s_1}s_2\tilde{s_2} + d_2\tilde{s_2}s_1\tilde{s_1} = \tilde{d_1}s_1s_2\tilde{s_2} + \tilde{d_2}s_2s_1\tilde{s_1} = (\tilde{d_1}\tilde{s_2}+\tilde{d_2}\tilde{s_1})(s_1s_2). \\ (d_1d_2)(\tilde{s_1}\tilde{s_2}) &= d_1\tilde{s_1}d_2\tilde{s_2} = \tilde{d_1}s_1\tilde{d_2}s_2 = (\tilde{d_1}\tilde{d_2})(s_1s_2). \end{aligned}$$

Por tanto $(d_1/s_1)+(d_2/s_2) = (\tilde{d_1}/\tilde{s_1})+(\tilde{d_2}/\tilde{s_2})$ y también $(d_1/s_1)\cdot(d_2/s_2) = (\tilde{d_1}/\tilde{s_1})\cdot(\tilde{d_2}/\tilde{s_2})$. Se comprueba de forma directa que $(F,+,\cdot)$ es cuerpo, que $0_F = 0_D/1_D$ es el elemento neutro de la suma, $1_F = 1_D/1_D$ es el elemento neutro del producto, $-d/s$ es el opuesto de d/s y si $d/s \neq 0_F$ su inverso para el producto es $(d/s)^{-1} = s/d$.
(I) Consideramos la aplicación $\Phi : D \to F$ dada por $\Phi(d) = d/1_D$ es un homomorfismo de anillos unitarios inyectivo. Por lo que, aplicando el primer teorema de isomorfía $D \approx \mathrm{Im}\Phi$ y, por la Propiedad II.3.3, se tiene que $\tilde{D} := \mathrm{Im}\Phi$ es un subanillo de F.
(II) Sea L un cuerpo con $\tilde{D} \subseteq L \subseteq F$. Dado $(d/s) \in F$ con $d \in D$ y $s \in S$, como $\tilde{D} \subseteq L$ tenemos que $d/1_D, s/1_D \in L$. Como $s/1_D \neq 0$ existe $(s/1_D)^{-1}$ y, como L es cuerpo, $(s/1_D)^{-1} \in L$. Resulta que, como L es cuerpo, $(d/1_D)(s/1_D)^{-1} \in L$ y concluimos que

$$\frac{d}{s} = \frac{d}{1_D}\frac{1_D}{s} = \frac{d}{1_D}\left(\frac{s}{1_D}\right)^{-1} \in L.$$

De modo que $F \subseteq L$ y $L = F$. ■

El teorema anterior, además de la existencia, garantiza la unicidad, salvo isomorfismo del cuerpo de fracciones

Definición II.4.18 Sea D un dominio. El cuerpo F construido en el Teorema II.4.17 se denota por $F(D)$ y se denomina **cuerpo de fracciones de** D.

Ejemplos II.4.19 (1) Si $\mathbb{K}$ es un cuerpo $\mathbb{K} \approx F(\mathbb{K})$.

(2) El cuerpo de fracciones de $(\mathbb{Z},+,\cdot)$ es $(\mathbb{Q},+,\cdot)$, es decir, $F(\mathbb{Z}) = \mathbb{Q}$.

(3) El cuerpo de fracciones de $(\mathbb{R}[x],+,\cdot)$ es el conjunto de fracciones racionales, es decir, $F(\mathbb{R}[x]) = \mathbb{R}(x)$ donde

$$\mathbb{R}(x) := \left\{\frac{P}{Q} : P,Q \in \mathbb{R}[x],\ Q \neq 0\right\} \qquad \textit{(Fracciones racionales con coeficientes reales).}$$

Ejercicio II.4.20 ¿Cuántos elementos tiene el anillo $(\mathbb{Z}/1\mathbb{Z},+,\cdot)$? ¿es conmutativo?¿es unitario?¿es un dominio?¿es un cuerpo?

Ejercicio II.4.21 (Anillos de división). Los anillos $(F,+,\cdot)$ que verifican (F.II) y (F.III) pero no necesariamente (F.I) se denominan **anillos de división**. ¿Podrías dar un ejemplo de un anillo $(F,+,\cdot)$ que satisfaga (F.II) y (F.III) pero no (F.I)? ¿y si adicionalmente imponemos que F es finito? Nota: Tras intentar buscar un contraejemplo de la segunda pregunta buscar información sobre el pequeño Teorema de Wedderburn.

Ejercicio II.4.22 Dados R,S dos anillos isomorfos. Probar que:

1. R es unitario si y solo si S es unitario.
2. R es conmutativo si y solo si S es conmutativo.
3. R es un dominio si y solo si S es un domino.
4. R es un cuerpo si y solo si R es un cuerpo

Demostrar que los anillos $\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Q}$, $12\mathbb{Z}$, $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$ no son isomorfos.

Ejercicio II.4.23 Dado R un anillos conmutativo y unitario, probar que

$$R \text{ satisface (D.III)} \quad \Leftrightarrow \quad 0_R \text{ es divisor de cero y se cumple la ley de cancelación en } R.$$

Ejercicio II.4.24 Dar un ejemplo de un anillo en el cual exista un elemento $a \neq 0$ que no sea ni divisor del 0 ni unidad.

Ejercicio II.4.25 Determinar todas las unidades y divisores del cero en $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Ejercicio II.4.26 Probar que $\mathbb{Z}[i]$ es un dominio de integridad. Determinar los elementos de $\mathbb{Z}[i]/(2)$ y $\mathbb{Z}[i]/(3)$ ¿alguno de estos anillos es dominio de integridad?

Ejercicio II.4.27 Si D es un dominio de integridad y se cumple que $20 \cdot 1_D = 12 \cdot 1_D$ ¿Cuál es la característica de D?

Ejercicio II.4.28 Determinar las soluciones de $x^2 + 6x - 31 \equiv 0 \,(\text{mód} 72)$

Ejercicio II.4.29 Probar que el ideal $((1,0))$ del anillo $\mathbb{Z} \times \mathbb{Z}$ es primo pero no es maximal. Encontrar un ideal maximal en $\mathbb{Z} \times \mathbb{Z}$.

Ejercicio II.4.30 Probar que $\left(x^2 - 2\right)$ es un ideal maximal en $\mathbb{Q}[x]$.

Ejercicio II.4.31 Probar que $\mathbb{Q}[\sqrt{6}] = \{a + b\sqrt{6} : a,b \in \mathbb{Q}\}$ es un cuerpo.

Ejercicio II.4.32 Consideramos las matrices de $Mat_{2\times 2}(\mathbb{C})$ dadas por

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Definimos el subconjunto $H = \{aI + bB + cC + dD : a,b,c,d \in \mathbb{R}\}$. Probar que H es un subanillo de $Mat_{2\times 2}(\mathbb{C})$. ¿Es H un cuerpo? Estudiar la relación con el Ejercicio I.2.22.

Ejercicio II.4.33 ¿Podrías dar otros dos ejemplos de dominios con sus respectivos cuerpos de fracciones distintos de los presentados en el Ejemplo II.4.19?

Ejercicio II.4.34 Dado D un dominio de integridad, $F(D)$ su cuerpo de fracciones y $\mathbb{K}$ un cuerpo. Entonces para cada homomorfismo de anillos unitarios $f: D \to \mathbb{K}$ inyectivo, existe un único monomorfismo $g: F \to \mathbb{K}$ tal que $g \circ \ell = f$, donde $\ell: D \to F(D)$ es el homomorfismo que envía d en $\frac{d}{1}$.

II.5 Dominios de factorización única, dominios de ideales principales y dominios euclídeos

II.5.1 Elementos irreducibles y elementos primos de un dominio

La noción de dominio generaliza de un modo más fiel las propiedades de $(\mathbb{Z}, +, \cdot)$ que la noción de anillo. Sin embargo, existen bastantes propiedades de $(\mathbb{Z}, +, \cdot)$ que no se satisfacen en cualquier dominio. Por ejemplo en $(\mathbb{Z}, +, \cdot)$ todo ideal primo es maximal y en $(\mathbb{Z}, +, \cdot)$ todo entero mayor que 1 factoriza de forma única como producto de primos (Teorema fundamental de la Aritmética). En esta sección vamos a ver cómo extender la descomposición en factores al contexto de los dominios.

Definición II.5.1 Sean D un domino de integridad y $a, b \in D$. Decimos que a y b son **asociados** si existe $u \in U(D)$ tal que $a = bu$ y lo representamos por $a \sim b$.

Proposición II.5.2 Sean D un domino de integridad y $a, b \in D$. Entonces

$$a \sim b \quad \Leftrightarrow \quad a \mid b \quad \text{y} \quad b \mid a.$$

Demostración. $(\Rightarrow)$ Si $a \sim b$, entonces existe $u \in U(D)$ tal que $a = bu$, luego $au^{-1} = b$. Por tanto, $a \mid b$ y $b \mid a$.
$(\Leftarrow)$ Si $a = 0_D$ como $a \mid b$, $b = 0_D$ y $a = 0_D \sim 0_D = b$. Si $b = 0_D$ como $b \mid a$, $a = 0_D$ y $a = 0_D \sim 0_D = b$. Finalmente, si $a, b \in D \backslash \{0_D\}$ y $a \mid b$ y $b \mid a$, existen $c, d \in D$ tales que $ac = b$ y $a = bd$. Por ello, $a = acd$ y $b = bdc$ y, por la Ley de cancelación, $1_D = cd$ y $1_D = dc$. En consecuencia, $c, d \in U(D)$ y $a \sim b$. ■

Ejemplos II.5.3 (1) Como $U(\mathbb{Z}) = \{-1, 1\}$, entonces para todo $a \in \mathbb{Z}$ los únicos asociados de a son a y $-a$.

(2) Dados $P(x) = 3x^2 + 6x$ y $Q(x) = x^2 + 2x$. Como $P(x) = 3Q(x)$ tenemos que P y Q son **asociados en** $\mathbb{Q}[x]$ porque $3 \in U(\mathbb{Q}[x])$.
Sin embargo, **no son asociados en** $\mathbb{Z}[x]$ porque $3 \notin U(\mathbb{Z}[x]) = \{-1, 1\}$.
Por otro lado, si los estudiamos como polinomios de $\mathbb{Z}/7\mathbb{Z}[x]$, ambos son asociados porque $3 \in U(\mathbb{Z}/7\mathbb{Z}[x]) = \{1, 2, 3, 4, 5, 6\}$. En resumen, la condición de ser asociados o no depende del anillo al que pertenezcan.

(3) Hemos visto que $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$ (ver Ejercicio II.1.27) luego 3, $3i$, -3 y $-3i$ son asociados en $\mathbb{Z}[i]$. De la misma forma, $2 + 3i$ y $-3 + 2i$ son asociados en $\mathbb{Z}[i]$.

Observación II.5.4 Se puede probar que a y b son son asociados si y sólo si $(a) = (b)$. (ver Ejercicio II.5.40).

Definición II.5.5 Sean D un domino de integridad y $a \in D\backslash\{0_D\}$ con $a \notin U(D)$, decimos que

(A) a es **irreducible** en D si tiene la siguiente propiedad:

si para todos $b,c \in D$ tal que $a = bc$ se tiene que $b \in U(D)$ o $c \in U(D)$.

(B) a es **primo** en D si tiene la siguiente propiedad:

si para todos $b,c \in D$ tal que $a \mid bc$ se tiene que $a \mid b$ o $a \mid c$.

Ejemplos II.5.6 (1) Como $U(\mathbb{Z}) = \{-1,1\}$, la definición general de primo, Definición II.5.5 y la definición particular en el caso de los enteros, Definición A.2.17 coinciden. En otras palabras, p es primo en $\mathbb{Z}$ por la Definición II.5.5 si y solo si es primo por la Definición A.2.17.
Por otro lado, en la Proposición A.2.20, hemos probado que dado $p \in \mathbb{Z}\backslash\{-1,0,1\}$ se tiene que p es primo en $\mathbb{Z}$ si y solo si p es irreducible en $\mathbb{Z}$. Este hecho no es cierto en dominios cualesquiera como veremos en esta sección.

(2) Queremos estudiar los elementos irreducibles y los primos de $\mathbb{C}$, pero tenemos que $U(\mathbb{C}) = \mathbb{C}\backslash\{0\}$ todos los elementos no nulos son unidades, luego ningún elemento cumple las hipótesis de la Definición II.5.5, luego no hay ni elementos irreducibles ni primos en $\mathbb{C}$.

En general si $\mathbb{K}$ es un cuerpo Como $U(\mathbb{K}) = \mathbb{K}\backslash\{0\}$ no hay ningún elemento con $a \neq 0$ y $a \notin U(\mathbb{K})$, luego no hay ni elementos irreducibles ni primos. Por tanto se trata de una noción que sólo tiene sentido para dominios D que no son cuerpos.

(3) 2 no es primo en $\mathbb{Z}[i]$. En primer lugar, comprobamos que $2 \neq 0$ y que $2 \notin U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. Por otro lado, observamos que $(1+i)(1-i) = 2$, luego $2 \mid (1+i)(1-i)$. Comprobamos que $2 \nmid (1+i)$ porque si $(1+i) = 2(a+bi)$ tendríamos que $a = b = 1/2$, lo que es imposible porque a y b deben ser enteros. De la misma forma vemos que $2 \nmid (1-i)$ y concluimos que 2 no es primo en $\mathbb{Z}[i]$.

(4) $P(x) = 3x$ es irreducible en $\mathbb{Q}[x]$, pero no es irreducible en $\mathbb{Z}[x]$.

(5) $P(x) = x^2 - 2$ es irreducible en $\mathbb{Q}[x]$, pero no es irreducible en $\mathbb{R}[x]$.

Observación II.5.7 Dado $a \in D\backslash\{0_D\}$ con $a \notin U(D)$ y $u \in U(D)$ se tiene que:

(A) a es irreducible si y solamente si au es irreducible.

(B) a es primo si y solamente si au es primo.

En otras palabras, las nociones de primo e irreducible son estables por la relación $\sim$.

Observación II.5.8 Dado $a \in D\backslash\{0_D\}$ con $a \notin U(D)$ y $a_1, a_2, \ldots a_n \in D$. Por el Principio de Inducción (ver TeoremaA.1.1) se puede probar que:

(A) Si a es irreducible y $a = a_1 a_2 \cdots a_n$, entonces
existe $j \in \{1,2,\ldots n\}$ tal que $a_j \notin U(D)$ y $a_i \in U(D)$ si $i \neq j$ con $i \in \{1,2,\ldots n\}$.

(B) Si a es primo y $a \mid a_1 a_2 \cdots a_n$, entonces existe $i \in \{1,2,\ldots n\}$ tal que $a \mid a_i$.

Proposición II.5.9 Sea D un dominio y $a \in D\backslash\{0_D\}$ con $a \notin U(D)$. Entonces tenemos que:

(I) a es primo si y sólo si (a) es un ideal primo.

(II) si a es primo, entonces a es irreducible.

Demostración. (I) $\boxed{\Rightarrow}$ Como $a \notin U(D)$ tenemos que $1_D \notin (a)$. Por tanto, $(a) \neq D$ luego (a) satisface (P.I).
Dados $b,c \in D$ con $bc \in (a)$ tenemos que $a \mid bc$ y, como a es primo, $a \mid b$ o $a \mid c$. Por consiguiente, $b \in (a)$ o $c \in (a)$, es decir, (a) satisface (P.II) y, por este motivo, (a) es un ideal primo.
$\boxed{\Leftarrow}$ Dados $b,c \in D$ tales que $a \mid bc$, se tiene que existe $r \in D$ de modo que $bc = ra$. De forma que $bc \in (a)$ y, por (P.II), se cumple que $b \in (a)$ o $c \in (a)$. Dicho de otro modo, $a \mid b$ o $a \mid c$, entonces a es primo.

(II) Supongamos que a es primo y que existen $b,c \in D$ tales que $a = bc$, entonces $a1_D = bc$, es decir, $a \mid bc$. Como a es primo $a \mid b$ o $a \mid c$. Supongamos que $a \mid b$, luego $ar = b$ para algún $r \in D$. Podemos escribir $a = rac$ y como $a \neq 0_D$, por la Ley de Cancelación, $rc = 1_D$, esto es, $c \in U(D)$. Análogamente si $a \mid c$, vemos que $b \in U(D)$ y concluimos que a es irreducible.

■

Ejemplo II.5.10 En general, el recíproco de la Proposición II.5.9.(II) no es cierto, es decir, en un dominio pueden existir elementos irreducibles que no son primos. Los anillos de la forma $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ no son muy útiles en el estudio de dominios de integridad que no son cuerpos porque como vimos en el Ejemplo II.4.8, o bien son cuerpos si n es primo o bien no son dominios para n no primo.
En este contexto, aparecen otros dominios (que no son cuerpos) y que nos van a servir para entender la noción de dominio de factorización única, que acabamos de introducir, y las de dominio de ideales principales y dominio euclídeo que veremos en las siguientes clases. Para $d \in \mathbb{N}_{\geq 1}$, consideramos los subconjuntos de $(\mathbb{R},+,\cdot)$ y $(\mathbb{C},+,\cdot)$ definidos por

$$\mathbb{Z}[\sqrt{d}] := \{a+b\sqrt{d} : a,b \in \mathbb{Z}\} \subseteq \mathbb{R}, \quad \text{(ver Ejercicio II.5.43)}$$
$$\mathbb{Z}[i\sqrt{d}] := \{a+bi\sqrt{d} : a,b \in \mathbb{Z}\} \subseteq \mathbb{C}. \quad \text{(ver Ejercicio II.5.42)}$$

(para $d = 1$, en el primer caso tenemos los enteros y en el segundo caso los enteros de Gauss). Mediante el test de caracterización de subanillos se prueba que son subanillos de $(\mathbb{R},+,\cdot)$ y $(\mathbb{C},+,\cdot)$, respectivamente. Comprobamos también que $(\mathbb{Z}[\sqrt{d}],+,\cdot)$ y $(\mathbb{Z}[i\sqrt{d}],+,\cdot)$ son dominios. Aunque estos dominios pueden parecer sencillos esconden propiedades singulares y complicadas de desentrañar.

Nuestro objetivo es probar que en el dominio $\mathbb{Z}[i\sqrt{5}] = \{a+bi\sqrt{5} : a,b \in \mathbb{Z}\}$ el elemento $1+i\sqrt{5}$ es irreducible pero no es primo. Para ellos vamos a hacer uso de las propiedades, probadas en el Ejercicio II.5.42, de la función $N : \mathbb{Z}[i\sqrt{5}] \to \mathbb{Z}$ que a cada elemento de $\mathbb{Z}[i\sqrt{5}]$ lo envía en su módulo complejo al cuadrado, es decir,

$$N(a+b\sqrt{5}i) = a^2 + b^2 5.$$

En primer lugar, veamos que $\alpha := 1+i\sqrt{5}$ **es irreducible en** $\mathbb{Z}[i\sqrt{5}]$. Supongamos que $\alpha = \beta\gamma$, por el Ejercicio II.5.42.(II), tenemos que $6 = N(\alpha) = N(\beta)N(\gamma)$. Como la función N toma valores en $\mathbb{N}$, podemos distinguir dos casos:

(a) $N(\beta)=1$ y $N(\gamma)=6$ (o $N(\beta)=6$ y $N(\gamma)=1$). En este caso, por el Ejercicio II.5.42.(III), tendríamos que β es una unidad (o que γ es una unidad). En consecuencia, $1+i\sqrt{5}$ **es irreducible en** $\mathbb{Z}[i\sqrt{5}]$.

(b) $N(\beta)=2$ y $N(\gamma)=3$ (o $N(\beta)=3$ y $N(\gamma)=2$). Veamos que este caso es imposible. Tenemos que las ecuaciones: $x^2+5y^2=2$ y $x^2+5y^2=3$ no tiene soluciones enteras. Por tanto, no puede existir un elemento $x+yi\sqrt{5}$ de $\mathbb{Z}[i\sqrt{5}]$, con $N(x+yi\sqrt{5})=2$ o con $N(x+yi\sqrt{5})=3$.

Por consiguiente, concluimos que $1+i\sqrt{5}$ es irreducible en $\mathbb{Z}[i\sqrt{5}]$.
Veamos que α **no es primo en** $\mathbb{Z}[i\sqrt{5}]$. Observamos que: $(1+i\sqrt{5}) \mid 6$ porque $(1+i\sqrt{5})(1-i\sqrt{5})=6$. Luego $(1+i\sqrt{5}) \mid 6$, es decir, $(1+i\sqrt{5}) \mid (2\cdot 3)$.
Veamos que $(1+i\sqrt{5}) \nmid 2$ y que $(1+i\sqrt{5}) \nmid 3$.
Supongamos que $(1+i\sqrt{5}) \mid 2$, es decir, $(1+i\sqrt{5})\beta=2$ para algún $\beta\in\mathbb{Z}[i\sqrt{5}]$. Por el Ejercicio II.5.42.(II) se tendría que $4=N(2)=N((1+i\sqrt{5})\beta)=6N(\beta)$. Sin embargo, esto es imposible porque $N(\beta)\in\mathbb{N}$. Por este motivo, $(1+i\sqrt{5}) \nmid 2$.
Análogamente, comprobamos que $(1+i\sqrt{5}) \nmid 3$.
Concluimos que $1+i\sqrt{5}$ es un elemento irreducible en $\mathbb{Z}[i\sqrt{5}]$ que no es primo en $\mathbb{Z}[i\sqrt{5}]$. En otras palabras, el recíproco de la Proposición II.5.9.(II) no es cierto.

II.5.2 Dominios de factorización única

Introducimos un tipo especial de dominios donde la descomposición única en elementos irreducibles es posible.

Definición II.5.11 Sea D un dominio decimos que D es un **dominio de factorización única (D.F.U.)** si

(DFU.I) cada elemento de no nulo y que no es una unidad se puede escribir como producto de irreducibles de D.

(DFU.II) si $p_1,p_2,\dots p_n$ y $q_1,q_2,\dots q_m$ son elementos irreducibles de D tales que

$$p_1p_2\cdots p_n=q_1q_2\cdots q_m,$$

entonces se cumple que $n=m$ y existe $\sigma\in S_n$ tal que para todo $i\in\{1,2,\cdots,n\}$ se tiene que $p_i\sim q_{\sigma(i)}$.

En la Proposición II.5.9, se ha probado que en un dominio todo elemento primo es irreducible. Como muestra el Ejemplo II.5.10, el recíproco no es cierto en general. Sin embargo, en dominios de factorización única son conceptos equivalentes.

Proposición II.5.12 Sea D un D.F.U. Todo elemento irreducible es primo.

Demostración. Dado $a\in D\backslash\{0_D\}$ con $a\notin U(D)$ un elemento irreducible. Dados $b,c\in D$ tales que $a \mid bc$, es decir, tales que existe $x\in D$ con $ax=bc$, distinguimos tres casos:

(a) Si $b\in U(D)$, entonces $c=ab^{-1}x$ y tenemos que $a \mid c$.
Si $c\in U(D)$, entonces $b=ac^{-1}x$ y tenemos que $a \mid b$.

(b) Si $b=0$, entonces $a0=0=b$ y tenemos que $a \mid b$.
Si $c=0$, entonces $a0=0=c$ y tenemos que $a \mid c$.

(c) Si $b,c\notin U(D)$ y $b,c\in D\backslash\{0_D\}$. Como D es D.F.U., por (DFU.I) podemos afirmar que $b=b_1b_2\cdots b_r$ y que $c=c_1c_2\cdots c_s$ con b_j,c_i irreducibles en D. Distinguimos dos subcasos:

(c.1) Si $x \in U(D)$ entonces, como a es irreducible, por la Observación II.5.7, $\widetilde{a} = ax$ es irreducible y $\widetilde{a} = b_1 b_2 \cdots b_r c_1 c_2 \cdots c_s$. Por la unicidad de la descomposición (DFU.II), se tiene que o existe $j \in \{1,2,\ldots,r\}$ tal que $\widetilde{a} \sim b_j$ o existe $i \in \{1,2,\ldots,s\}$ tal que $\widetilde{a} \sim c_i$. Por tanto, existe $u \in U(D)$ tal que $b = b_1 b_2 \cdots b_{j-1}(axu)b_{j+1} \cdots b_r$ o $c = c_1 c_2 \cdots c_{i-1}(axu)c_{i+1} \cdots c_s$ y concluimos que $a \mid b$ ó $a \mid c$.

(c.2) Si $x \notin U(D)$ como $b, c \in D \backslash \{0_D\}$ se tiene que $x \in D \backslash \{0_D\}$. Por (DFU.I) podemos afirmar que $x = x_1 x_2 \cdots x_t$ con x_i irreducibles en D y se cumple que $ax_1 x_2 \cdots x_t = b_1 b_2 \cdots b_r c_1 c_2 \cdots c_s$. Como a es irreducible, por la unicidad de la descomposición (DFU.II), se tiene que o existe $j \in \{1,2,\ldots,r\}$ tal que $a \sim b_j$ o existe $i \in \{1,2,\ldots,s\}$ tal que $a \sim c_i$. Del mismo modo, concluimos que $a \mid b$ ó $a \mid c$.

En todos los casos hemos visto que $a \mid b$ ó $a \mid c$, es decir, a es primo. ■

Ejemplos II.5.13 (1) $\mathbb{Z}$ es un D.F.U. (Teorema fundamental de la Aritmética (TeoremaA.2.21)).

(2) $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ y $(\mathbb{Z}/p\mathbb{Z})[x]$ con $p \in \mathbb{N}_{\geq 1}$ primo son D.F.U. (Como probaremos detalladamente en la Sección II.6).

(3) $\mathbb{Z}/21\mathbb{Z}$ no es un D.F.U. porque no es un dominio.

(4) Por el Ejemplo II.5.10, existe un elemento irreducible que no es primo en $\mathbb{Z}[i\sqrt{5}]$, $1+i\sqrt{5}$, y, por la Proposición II.5.12, $\mathbb{Z}[i\sqrt{5}]$ es un dominio que no es un dominio de factorización única.

Nota: Podemos probar que $\mathbb{Z}[i\sqrt{5}]$ no es un dominio de factorización única de forma directa, porque 6 factoriza de dos formas distintas como producto de irreducibles no asociados entre ellos: $6 = 2 \cdot 3$ *y* $6 = (1+i\sqrt{5})(1-i\sqrt{5})$.

II.5.3 M.C.D. y M.C.M en dominios de factorización única

La existencia de una factorización única nos permite extender las nociones que conocemos en $(\mathbb{Z}, +, \cdot)$ de máximo común divisor y mínimo común múltiplo a un D.F.U. cualquiera.

Definición II.5.14 Sean D un dominio y a, b elementos de D, decimos que un elemento d de D es **un máximo común divisor de** a **y** b si

(MCD.I) se tiene que $d \mid a$ y $d \mid b$. (*Divisor común*)

(MCD.II) para todo $c \in D$ tal que $c \mid a$ y $c \mid b$ se cumple que $c \mid d$.
(*Máximo para la relación de divisibilidad*)

Ejemplos II.5.15 (1) De acuerdo con esta definición 12 y -12 son dos máximos comunes divisores de 36 y 24 en $\mathbb{Z}$. Como se detalló en la Notación A.2.8, para evitar la dualidad se elige del máximo común divisor en $\mathbb{N}$.

(2) En $\mathbb{R}[x]$, dados los polinomios $P(x) = 4x^4 - 4$ y $Q(x) = 2x^3 + x^2 + 2x + 1$, como $P(x) = 4\left(x^2+1\right)(x+1)(x-1)$ y como $Q(x) = (2x+1)\left(x^2+1\right)$ tenemos que un máximo común divisor es $D(x) = (x^2+1)$, pero también son máximos comunes divisores

$$2(x^2+1), \qquad \frac{1}{2}(x^2+1), \qquad \sqrt{3}(x^2+1), \qquad \pi(x^2+1).$$

En general, cualquier polinomio de la forma $r(x^2+1)$ con $r \in \mathbb{R}$ es un máximo común divisor de $P(x)$ y $Q(x)$, es decir, hay infinitas posibilidades. En el contexto de polinomios con coeficientes en un cuerpo, para garantizar la unicidad se suele elegir el polinomio mónico como máximo común divisor.

Definición II.5.16 Sean D un dominio y a,b elementos de D, decimos que un elemento m de D es **un mínimo común múltiplo de** a **y** b si

(MCM.I) se tiene que $a \mid m$ y $b \mid m$. (*Múltiplo común*)

(MCM.II) para todo $n \in D$ tal que $a \mid n$ y $b \mid n$ se cumple que $m \mid n$. (*Mínimo para la relación de divisibilidad*)

Observación II.5.17 Si d y $\widetilde{d}$ son dos máximos comunes divisores de a y b, entonces $d \sim \widetilde{d}$. Si m y $\widetilde{m}$ son dos mínimos comunes múltiplos de a y b, entonces $m \sim \widetilde{m}$.
Por consiguiente, el máximo común divisor y el mínimo común múltiplo son únicos salvo producto por unidades, es decir, módulo la relación de equivalencia $\sim$ (ver Ejercicio II.5.39), o en otras palabras, son únicos en $D/\sim$.

Para probar que en todo D.F.U. siempre existen el máximo común divisor y existe el mínimo común múltiplo, vamos a emplear el siguiente lema auxiliar.

Lema II.5.18 — Reordenación de factores. Sean D un D.F.U. y $a \in D\backslash\{0_D\}$ con $a \notin U(D)$. Entonces existen $p_1, p_2, \ldots, p_m$ elementos irreducibles de D con $p_i \not\sim p_j$ si $i \neq j$, $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{N}_{\geq 1}$ y $u \in U(D)$ tales que

$$a = u p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}.$$

Demostración. Por por (DFU.I), podemos afirmar que $a = a_1 a_2 \cdots a_r$ con a_i irreducibles en D. En el conjunto $A = \{a_1, a_2, \ldots, a_r\}$ consideramos la relación de equivalencia $\sim$ (ver Ejercicio II.5.39). Escribimos $m := \#(A/\sim)$, es decir, $m \in \mathbb{N}_{\geq 1}$ es el número de clases de equivalencia de $(A/\sim) = \{P_1, P_2, \ldots, P_m\}$. Para todo $j \in \{1,2,\ldots,m\}$, denotamos por $\alpha_j := \#P_j$ y elegimos un representante p_j de la clase P_j. Como las clases de equivalencia son disjuntas $p_i \not\sim p_j$ si $i \neq j$. Para todo $j \in \{1,2,\ldots,m\}$ y para todo $a_k \in P_j$ tenemos que $a_k = h_k p_j$ con $h_k \in U(D)$, entonces definimos $u_j := \prod_{a_k \in P_j} h_k$. Con esta notación y empleando la propiedad conmutativa del producto vemos que

$$a = a_1 a_2 \cdots a_r = u_1 p_1^{\alpha_1} u_2 p_2^{\alpha_2} \cdots u_m p_m^{\alpha_m} = u p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m},$$

donde $u = \prod_{j=1}^{m} u_j$ que es una unidad (Propiedad II.1.15.v). ■

Proposición II.5.19 Sean D un D.F.U. y $a,b \in D$. Entonces existe al menos un máximo común divisor de a y b y al menos un mínimo común múltiplo de a y b.

Demostración. Si $a \in U(D)$, o $b \in U(D)$ o $a = 0_D$ o $b = 0_D$, entonces se puede probar la existencia de al menos un máximo común divisor de a y b y al menos un mínimo común múltiplo de a y b, sin necesidad de emplear la factorización, ver Ejercicio II.5.47 y Ejercicio II.5.48.
Por consiguiente, supondremos que $a,b \notin U(D)$ y que $a,b \in D\backslash\{0\}$. En este caso, tenemos que $ab \notin U(D)$ porque $a,b \notin U(D)$. Como D es un D.F.U., por el Lema II.5.18, podemos afirmar que $ab = w p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ con p_i irreducibles en D, $w \in U(D)$ y $\gamma_i \in \mathbb{N}_{\geq 1}$. Por (DFU.II), se cumple que

$$a = u_1 p_1^{\alpha_1} u_2 p_2^{\alpha_2} \cdots u_m p_n^{\alpha_n} = u p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$
$$b = v_1 p_1^{\beta_1} v_2 p_2^{\beta_2} \cdots v_n p_n^{\beta_n} = v p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n},$$

con $\alpha_i, \beta_i \in \mathbb{N}$ y $u = \prod_{j=1}^{m} u_j$ y $v = \prod_{j=1}^{m} v_j$. Para todo $i \in \{1,2,\ldots,n\}$ definimos $\delta_i := \text{mín}(\alpha_i, \beta_i)$ y $\mu_i := \text{máx}(\alpha_i, \beta_i)$ y consideramos

$$d := p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n} \quad \text{y} \quad m := p_1^{\mu_1} p_2^{\mu_2} \cdots p_n^{\mu_n}.$$

Comprobamos de forma directa que d es máximo común divisor de a y b y que m es un mínimo común múltiplo de a y b. Por tanto, observamos que en un D.F.U., se verifica la definición usual en $\mathbb{Z}$, usual: el máximo común divisor son los factores irreducibles comunes elevados al mínimo exponente (si no son comunes $\delta_i = 0$) y el mínimo común múltiplo son los factores irreducibles comunes y no comunes elevados al máximo exponente. ■

Observación II.5.20 Para definir el máximo común divisor y el mínimo común múltiplo de un conjunto finito $X = \{x_1, x_2, \ldots x_r\}$ de elementos de D podemos proceder de **forma recursiva**: decimos que $d \in D$ es un máximo común divisor de $x_1, x_2, \ldots x_{r-1}, x_r$ si d es un máximo común divisor de d_{r-1} y x_r donde d_{r-1} es un máximo común divisor de $x_1, x_2, \ldots x_{r-1}$. Análogamente $m \in D$ es un mínimo común múltiplo de $x_1, x_2, \ldots x_{r-1}, x_r$ si m es un mínimo común múltiplo de m_{r-1} y x_r donde m_{r-1} es mínimo común múltiplo de $x_1, x_2, \ldots x_{r-1}$.

No obstante, también podemos definir estas nociones de **forma axiomática**: Un elemento d de D es un máximo común divisor de $x_1, x_2, \ldots x_{r-1}, x_r$ si

(MCD.I) para todo $x \in X$ se tiene que $d \mid x$.

(MCD.II) para todo $c \in D$ tal que para todo $x \in X$ se tiene que $c \mid x$, se cumple que $c \mid d$.

Un elemento m de D es un mínimo común múltiplo de $x_1, x_2, \ldots x_{r-1}, x_r$ si

(MCM.I) para todo $x \in X$ se tiene que $x \mid m$.

(MCM.II) para todo $n \in D$ tal que para todo $x \in X$ se tiene que $x \mid n$, se cumple que $m \mid n$.

Se puede comprobar que ambas definiciones coinciden.

II.5.4 Dominios de ideales principales

En el anillo $(\mathbb{Z}, +, \cdot)$ todo ideal está generado por un único elemento. Veamos como formalizar esta propiedad para dominios cualesquiera.

Definición II.5.21 Sea $(R, +, \cdot)$ un anillo, un ideal I se dice que es **principal** si existe $a \in R$ tal que $I = (a)$.

Definición II.5.22 Sea D un dominio de integridad, decimos que es un **dominio de ideales principales (D.I.P.)** cuando todo ideal de D es principal, es decir, todo ideal está generado por un elemento.

Ejemplos II.5.23 (1) $\mathbb{Z}$ es un D.I.P. (ver Ejercicio II.2.20)

(2) $\mathbb{Z}[x]$ no es un D.I.P. porque $(2,x)$ no es principal. Razonando por reducción al absurdo si $(2,x) = (P(x))$ con $P(x) \in \mathbb{Z}[x]$ tendríamos que $2 \in (P(x))$, luego $P(x) \mid 2$ y por ellos $P(x) \in \{\pm 1, \pm 2\}$. Como $x \notin (2) = (-2)$, necesariamente $P(x) = \pm 1$. Sin embargo, $\pm 1 \notin (2,x)$ porque los elementos del ideal $(2,x)$ son los polinomios con término independiente par (ver Ejercicio II.4.12). En consecuencia, $(2,x)$ no puede ser expresado como el ideal generado por un único elemento de $\mathbb{Z}[x]$.

En primer lugar, vamos a probar que en un D.I.P. toda sucesión creciente de ideales es estacionaria.
Nota: Los anillos conmutativos con esta propiedad se conocen como ***anillos Noetherianos****.*

Proposición II.5.24 Sean D un D.I.P. y $(I_n)_{n=1}^{\infty}$ una sucesión de ideales de D tal que para todo $n \in \mathbb{N}_{\geq 1}$ se cumple que $I_n \subseteq I_{n+1}$. Entonces:

(I) $I := \cup_{n=1}^{\infty} I_n$ es un ideal.

(II) existe $n_0 \in \mathbb{N}_{\geq 1}$ tal que para todo $n \geq n_0$ se tiene que $I_n = I_{n_0}$.

Demostración. (I) Dados $x, y \in I = \cup_{n=1}^{\infty} I_n$ y $r \in D$ se tiene que existen $n_1, n_2 \in \mathbb{N}_{\geq 1}$ tales que $x \in I_{n_1}$, $y \in I_{n_2}$. Si $N := \text{máx}(n_1, n_2)$, como la sucesión de ideales es creciente, tenemos que $x, y \in I_N$. Como I_N es ideal $x - y \in I_N$ y $rx, xr \in I_N$, luego $x - y \in I$ y $rx, xr \in I$. En consecuencia por el test de caracterización de ideales I es un ideal.
(Nota: Este apartado es cierto en cualquier anillo R)

(II) Como D es un D.I.P. y, por (I), I es un ideal, tenemos que existe $a \in D$ tal que $I = (a)$. Como $a \in I$ tenemos que $a \in \cup_{n=1}^{\infty} I_n$ por lo tanto existe $n_0 \in \mathbb{N}_{\geq 1}$ tal que $a \in I_{n_0}$. Como I_{n_0} es ideal se tiene que $(a) \subseteq I_{n_0}$. En consecuencia, para todo $n \geq n_0$, como la sucesión de ideales es creciente, se cumple que

$$(a) \subseteq I_{n_0} \subseteq I_n \subseteq \cup_{n=1}^{\infty} I_n = I = (a).$$

En otras palabras, para todo $n \geq n_0$ se tiene que $I_n = I_{n_0} = I = (a)$. ■

En los D.I.P. el recíproco de la Proposición II.5.9.(II) también es cierto, es decir, todo elemento irreducible es primo. Además, en un D.I.P. todo ideal primo es maximal, propiedad que no es cierta en los D.F.U.

Proposición II.5.25 Sean D un D.I.P. y $a \in D \backslash \{0_D\}$ con $a \notin U(D)$. Son equivalentes:

(I) a es irreducible.

(II) (a) es maximal.

(III) (a) es primo.

(IV) a es primo.

Demostración. $\boxed{\text{(I)} \Rightarrow \text{(II)}}$ Como $a \notin U(D)$ tenemos que $1_D \notin (a)$. Por tanto, $(a) \neq D$ luego (a) satisface (M.I).
Dado J un ideal de D con $(a) \subseteq J \subseteq D$, como D es un D.I.P., existe $b \in D$ tal que $J = (b)$. Entonces $a \in (b)$ y existe $c \in D$ tal que $a = bc$. Como a es irreducible, b es una unidad o c es una unidad. En el primer caso, tenemos que $J = (b) = D$. En el segundo caso, tenemos que $a \sim b$ y, por el Ejercicio II.5.40, deducimos que $(a) = (b) = J$. En otras palabras, (a) satisface (M.II) y, por este motivo, (a) es un ideal maximal.
$\boxed{\text{(II)} \Rightarrow \text{(III)}}$ Directo por la Proposición II.4.13.
$\boxed{\text{(III)} \Rightarrow \text{(IV)}}$ Directo por la Proposición II.5.9.(I).
$\boxed{\text{(IV)} \Rightarrow \text{(I)}}$ Directo por la Proposición II.5.9.(II). ■

Los D.F.U. y los D.I.P. tienen tantas propiedades en común porque como muestra el resultado principal de esta sección todo D.I.P. es un D.F.U.

Teorema II.5.26 Todo dominio de ideales principales es un dominio de factorización única.

Demostración. **EXISTENCIA DE LA DESCOMPOSICIÓN (DFU.I)**

Dado $a \in D\backslash\{0_D\}$ y $a \notin U(D)$. Veamos que a descompone como producto de irreducibles.

(I) **Veamos que a tiene algún factor irreducible.**

Si a es irreducible hemos terminado. Si a no es irreducibles $a = b_1a_1$ con $b_1, a_1 \notin U(D)$. Como $a \neq 0_D$ tenemos que $b_1, a_1 \in D\backslash\{0_D\}$. Si a_1 es irreducible hemos terminado. Si a_1 no es irreducible $a_1 = b_2a_2$ con $b_2, a_2 \notin U(D)$ no nulos. Iterando el proceso, si para todo $n \in \mathbb{N}_{\geq 1}$, a_n no es irreducible, construimos dos sucesiones de elementos $\{a_n\}_{n=1}^{\infty}$ y $\{b_n\}_{n=1}^{\infty}$, que no son ni unidades ni nulos con $a_n = b_{n+1}a_{n+1}$. Por tanto, la correspondiente sucesión de ideales $\{(a_n)\}_{n=1}^{\infty}$ cumple que $(a_n) \subseteq (a_{n+1})$ para todo $n \in \mathbb{N}_{\geq 1}$. Por la Proposición II.5.24, existe $n_0 \in \mathbb{N}_{\geq 1}$ tal que $(a_n) = (a_{n_0})$ para todo $n \geq n_0$. En particular para $n = n_0 + 1$, tendríamos, por el Ejercicio II.5.40, que $a_{n_0+1} \sim a_{n_0}$, es decir que $a_{n_0} = ua_{n_0+1}$ con $u \in U(D)$. Sin embargo, por construcción sabemos que $a_{n_0} = b_{n_0+1}a_{n_0+1}$, es decir, por la Ley de Cancelación tendríamos que $b_{n_0+1} = u \in U(D)$, lo que contradice nuestra hipótesis sobre b_{n_0+1}. Consecuentemente, existe $k \in \mathbb{N}_{\geq 1}$ tal que a_k es irreducible y a tiene algún factor irreducible.

(II) **Veamos que a es producto de irreducibles.**

Si a es irreducible hemos terminado. Si a no es irreducible, por (I), existe p_1 irreducible tal que $a = p_1c_1$ con $c_1 \notin U(D)$, $c_1 \neq 0$. Si c_1 es irreducible hemos terminado. Si c_1 no es irreducible, aplicando el apartado (I) a c_1 existe p_2 irreducible tal que $c_1 = p_2c_2$ con $c_2 \notin U(D)$, $c_2 \neq 0$. Razonando del mismo modo que en el apartado (I), pero esta vez considerando la sucesión de ideales $\{(c_n)\}_{n=1}^{\infty}$, concluimos que existe $k \in \mathbb{N}_{\geq 1}$ tal que c_k es irreducible y a se escribe como $a = p_1p_2\cdots p_kc_k$, es decir, como producto de irreducibles.

UNICIDAD DE LA DESCOMPOSICIÓN (DFU.II)

Dados p_i, q_j con $i, j \in \mathbb{N}_{\geq 1}$ elementos irreducibles en D, demostremos por inducción sobre n que:

$$\begin{array}{c} \forall m \in \mathbb{N}_{\geq 1} \quad \text{si} \quad p_1p_2\cdots p_n = q_1q_2\cdots q_m \\ \Downarrow \\ n = m \quad \text{y} \quad \exists \sigma \in S_n \quad \text{tal que} \quad \forall i \in \{1,2,\ldots,n\} \quad p_i \sim q_{\sigma(i)}. \end{array}$$

Veamos que se cumple si $n = 1$, es decir, si $p_1 = q_1q_2\cdots q_m$. Como p_1 es irreducible, la única forma de que descomponga como un producto es que alguno de los elementos sea una unidad (Observación II.5.8). Sin embargo, como para todo $j \in \{1,2,\ldots,m\}$ se tiene que q_j es irreducible, por definición, sabemos que $q_j \notin U(D)$. Por consiguiente, la única posibilidad es que $m = 1$, y deducimos que $n = m = 1$ y que $p_1 = q_1$, es decir, se cumple la propiedad.

Supongamos que se cumple la propiedad para un cierto $n \in \mathbb{N}_{\geq 1}$ y veamos que se cumple para $n+1$. Tenemos que $p_1p_2\cdots p_np_{n+1} = q_1q_2\cdots q_m$ con p_i, q_j irreducibles en D. Como D es un D.I.P. y p_{n+1} es irreducible, por la Proposición II.5.25, sabemos que p_{n+1} es primo y como $p_{n+1} \mid (q_1q_2\cdots q_m)$ sabemos por el Observación II.5.8 que $p_{n+1} \mid q_j$ para algún $j \in \{1,2,\ldots,m\}$. En consecuencia, existe $c \in D$ tal que $p_{n+1}c = q_j$. Como q_j es irreducible y como $p_{n+1} \notin U(D)$, deducimos que $c \in U(D)$ y que $p_{n+1} \sim q_j$. En otras palabras, podemos reescribir la igualdad como $p_1p_2\cdots p_np_{n+1} = q_1q_2\cdots q_{j-1}(cp_{n+1})q_{j+1}\cdots q_m$. Como $p_{n+1} \neq 0$, por la Ley de Cancelación, deducimos que $\widetilde{p}_1p_2\cdots p_n = q_1q_2\cdots q_{j-1}q_{j+1}\cdots q_m$ donde $\widetilde{p}_1 := c^{-1}p_1$ que es irreducible (Observación II.5.7).

Aplicando la **hipótesis de inducción**, sabemos que $n = m-1$ y que existe τ biyectiva de $\{1,2,\ldots,n\}$ en $\{1,2,\ldots,j-1,j+1,\ldots,m\}$ biyectiva tal que $p_i \sim q_{\tau(i)}$ para todo $i \in \{1,2,\ldots,n\}$. Definimos la permutación $\sigma : \{1,2,\ldots,n+1\} \to \{1,2,\ldots,n+1\}$ por $\sigma(i) = \tau(i)$ si $i \neq n+1$ y $\sigma(n+1) = j$. Con esta notación $n+1 = m$, $\sigma \in S_{n+1}$ y para todo $i \in \{1,2,\ldots,n+1\}$ se tiene que $p_i \sim q_{\sigma(i)}$ y la propiedad se satisface para $n+1$.

En consecuencia, por el Principio de Inducción queda demostrado que para todos $m,n \in \mathbb{N}_{\geq 1}$ si se cumple que $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ se tiene que $n = m$ y que existe $\sigma \in S_n$ tal que $p_i \sim q_{\sigma(i)}$ para todo $i \in \{1,2,\ldots,n\}$. En resumen, D verifica (DFU.II) y concluimos que D es un D.F.U. ■

Ejemplo II.5.27 El recíproco no es cierto $\mathbb{Z}[x]$ es un dominio de factorización única como probaremos en la Sección II.6 que no es un dominio de ideales principales (ver Ejemplo II.5.23)

Como todo D.I.P. es D.F.U., todas las propiedades probadas para D.F.U. son ciertas para D.I.P. En particular, las nociones de máximo común divisor y mínimo común múltiplo introducidas en la subsección anterior tienen perfecto sentido en un D.I.P. y podemos extender las relaciones entre ideales que conocemos en $(\mathbb{Z},+,\cdot)$.

Proposición II.5.28 — Ejercicio II.5.50. Sea D un D.I.P. y $a,b,d,m \in D$. Entonces:

(I) $(a)+(b) = (d)$ si y sólo si d es un máximo común divisor de a y b.
(*Identidad de Bezout*)

(II) $(a) \cap (b) = (m)$ si y sólo si m es un mínimo común múltiplo de a y b.

Nota: De acuerdo con la Proposición II.2.11 y la Observación II.2.9 se tiene que $(a)+(b) = ((a) \cup (b)) = (a,b)$.

II.5.5 Dominios euclídeos

Definición II.5.29 Sea D un dominio. Decimos que D es un **dominio euclídeo (D.E.)** si existe una aplicación $\delta : D\backslash\{0_D\} \to \mathbb{N}$ con las siguientes propiedades:

(DE.I) Para todos $a,b \in D\backslash\{0_D\}$ se tiene que $\delta(a) \leq \delta(ab)$.

(DE.II) Para todos $a,b \in D$ con $b \neq 0_D$ existen $q,r \in D$ tales que
$$a = bq + r \text{ con } \delta(r) < \delta(b) \quad \text{ó} \quad r = 0.$$

Ejemplos II.5.30 (1) $\mathbb{Z}$ **es un dominio euclídeo respecto al valor absoluto** $\delta(m) = |m|$**.**

Veamos que se cumple (DE.I)

Por las propiedades del valor absoluto sabemos que para todos $m,n \in \mathbb{Z}$ se tiene que $|nm| = |m||n|$ y que $|n| = 0$ si y sólo si $n = 0$.
Por lo tanto, dados $a,b \in \mathbb{Z}\backslash\{0\}$, se tiene que $|b| \geq 1$, luego $\delta(a) = |a| \leq |a||b| = |ab| = \delta(ab)$. En otras palabras, se satisface (DE.I).

Se cumple (DE.II): Demostrado en el Teorema A.2.3.

(2) Si F es un cuerpo, entonces el anillo de polinomios $F[x]$ es un dominio euclídeo respecto a la función $\delta(P(x)) = \text{gr}(P(x))$ (ver Teorema II.6.34).

(3) $\mathbb{Z}[i]$ es un dominio euclídeo respecto a la función $N(a+bi) = a^2+b^2$. (ver Ejercicio II.5.52)

Observación II.5.31 Las condiciones (DE.I) y (DE.II) no garantizan la unicidad del cociente y el resto. Para garantizar la unicidad es necesario que la función δ verifique alguna condición adicional, ver Ejercicio II.5.55. En el caso particular de los números enteros, si no imponemos ninguna condición adicional es posible realizar dos divisiones una con resto negativo y otra con resto positivo. Por ejemplo, que podemos dividir $a = 22$ entre $b = 3$ de dos formas distintas de acuerdo con (DE.II):

$$\begin{array}{lll} 22 = 7(3)+1 & \text{con} & q = 7, \quad r = 1, \quad \text{y} \quad |r| = 1 < 3 = |b|, \\ 22 = 8(3)+(-2) & \text{con} & q = 8, \quad r = -2, \quad \text{y} \quad |r| = 2 < 3 = |b|. \end{array}$$

Proposición II.5.32 Sea (D,δ) un dominio euclídeo. Entonces:

(I) $u \in U(D)$ si y sólo si $\delta(u) = \delta(1_D)$. (Ejercicio II.5.53)

(II) Si $a \sim b$, entonces $\delta(a) = \delta(b)$. (Ejercicio II.5.54)

El resultado principal de esta sección establece que todo D.E. es un D.I.P.

Teorema II.5.33 Todo dominio euclídeo es un dominio de ideales principales.

Demostración. Dado I un ideal de un dominio euclídeo (D,δ) veamos que está generado por un único elemento.
Si $I = \{0\}$ tenemos que $I = (0)$ y hemos terminado.
Si $I\backslash\{0\} \neq \emptyset$, consideramos $X := \{\delta(x) : x \in I\backslash\{0\}\} \subseteq \mathbb{N}$. Tenemos que $X \neq \emptyset$, luego por el **Principio de Buena Ordenación** existe $\delta_0 = \text{mín}(X)$. Sea $b \in I$ tal que $\delta(b) = \delta_0$.
Veamos que $I = (b)$. Como $b \in I$, tenemos que $(b) \subseteq I$. Veamos ahora que $I \subseteq (b)$. Dado $a \in I$, como (D,δ) es un dominio euclídeo y $b \neq 0$, existen $q,r \in D$ tales que $a = bq + r$ con $\delta(r) < \delta(b)$ o con $r = 0$. Como I es un ideal, se tiene que $bq \in I$, luego $r = a - bq \in I$. Dado que $\delta(b) = \delta_0 = \text{mín}(X)$, es imposible que se tenga que $\delta(r) < \delta(b)$, por ese motivo $r = 0$. En consecuencia, $a = bq$ y se cumple que $a \in (b)$. Por esta razón, $I \subseteq (b)$, concluimos que $I = (b)$.
En resumen, se cumple que D es un D.I.P. ■

Observación II.5.34 Por el Teorema II.5.26 y por el Teorema II.5.33, vemos que

$$\{\text{D. euclídeos}\} \subseteq \{\text{D. de ideales principales}\} \subseteq \{\text{D. de factorización única}\} \subseteq \{\text{Dominios}\}.$$

Todas estos contenidos son estrictos, $\mathbb{Z}[i\sqrt{5}]$ es un dominio que no es D.F.U. (ver Ejemplo II.5.13). El anillo de los polinomios con coeficientes enteros $\mathbb{Z}[x]$ es un D.F.U. que no es un D.I.P. Finalmente, cabe destacar que hasta 1949 no se conocía un D.I.P. que no fuera D.E. El ejemplo considerado proporcionado T. S. Motzkin es el dominio

$$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \left\{a+b\left(\frac{1+i\sqrt{19}}{2}\right) : a,b \in \mathbb{Z}\right\}.$$

Tenéis desglosada en la lista de ejercicios la prueba de que $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ es un D.I.P. que no es un D.E. siguiendo el artículo de O.A. Campoli de 1988 [4].

Como todo dominio euclídeo es un dominio de factorización única es posible definir el máximo común divisor de dos elementos. Adicionalmente, en un dominio euclídeo disponemos de un algoritmo que nos permite calcular un m.c.d. de dos elementos, sin necesidad de conocer su factorización en irreducibles: **el Algoritmo de Euclides**. La siguiente proposición garantiza que el algoritmo finaliza con éxito.

Proposición II.5.35 Sean (D,δ) un dominio euclídeo y a,b,d elementos de D con $b\neq 0$. Si $q,r\in D$ son los elementos dados por la propiedad (D.E.II), es decir, tales que $a=bq+r$, entonces tenemos que

d es un máximo común divisor de a y b si y sólo si d es máximo común divisor de b y r.

Demostración. Supongamos que d es un m.c.d. de a y b. Por (MCD.I) sabemos que $d \mid a$ y que $d \mid b$. Como $r=a-bq$, deducimos que $d \mid r$, es decir, d satisface (MCD.I) para b y r.
Dado $c\in D$ tal que $c \mid b$ y $c \mid r$. Como $a=bq+r$ vemos que $c \mid a$. Como d es un m.c.d. de a y b y como $c \mid a$ y $c \mid b$, por (MCD.II) se tiene que $c \mid d$, en otras palabras, d satisface (MCD.II) para b y r. Análogamente, si suponemos que d es un m.c.d. de b y r, concluimos que d es un m.c.d. de a y b. ■

ALGORITMO DE EUCLIDES

Entrada: Elementos a y b pertenecientes a un dominio euclídeo.

Salida: Un máximo común divisor d de a y b.

1. $r_0 := a$ y $r_1 := b$.
2. $i \leftarrow 1$.
3. Mientras $r_i \neq 0$ hacer:
   - **3.1.** Aplicar (D.E.II) a r_{i-1} y r_i para obtener q_i y r_{i+1} con $r_{i-1}=r_iq_i+r_{i+1}$.
   - **3.2.** $i \leftarrow i+1$.
4. La salida es: r_{i-1}.

Como cada vez que aplicamos el paso **3.1** tenemos que o bien $\delta(r_{i+1})<\delta(r_i)$ o bien $r_{i+1}=0$ podemos asegurar existe un $n\in\mathbb{N}_{\geq 1}$ de modo que el algoritmo termina en n pasos. Empleando la Definición II.5.14, se prueba que para todo $a\in D$ un m. c. d. entre a y 0_D es a. Cuando el algoritmo termina, se cumple que $r_n=0$, luego un m. c. d. entre r_{n-1} y r_n es r_{n-1}. Gracias a la Proposición II.5.35, sabemos que d es un m. c. d. de r_{i-1} y r_i si y solo si d es m. c. d. de r_{i-2} y r_{i-1}. Por consiguiente, como r_{n-1} es un m. c. d. de r_{n-1} y r_n, tenemos que r_{n-1} es un m. c. d. de a y b. En otras palabras, el Algoritmo de Euclides da finaliza de forma correcta y el **último resto no nulo** r_{n-1} es un m. c. d. de a y b.

Ejemplo II.5.36 En $\mathbb{Z}[i]$ queremos calcular un máximo común divisor de $\alpha=11+3i$ y $\beta=1+8i$. Realizamos la división en $\mathbb{C}$ de la forma habitual

$$z_1=\frac{11+3i}{1+8i}=\frac{(11+3i)(1-8i)}{65}=\frac{35}{65}-\frac{85}{65}i=\frac{7}{13}-\frac{17}{13}i.$$

Elegimos el elemento de $\mathbb{Z}[i]$ más próximo a $z_1=(7/13)-(17/13)i$ (ver Figura II.1), en realidad es posible elegir cualquiera de los vértices del cuadrado que contiene a z_1 (El resto y el cociente no son únicos). En consecuencia, tomamos como cociente $q_1=1-i$ dicho entero operando tenemos que:

$$(11+3i)=(1-i)(1+8i)+(2-4i).$$

Por lo tanto, el resto es $r_1=2-4i$, observamos que $N(r_1)=20$ y $N(\beta)=65$, luego la división es correcta. Repetimos el proceso y dividimos β entre r_1:

$$z_2=\frac{1+8i}{2-4i}=\frac{(1+8i)(2+4i)}{20}=\frac{-30}{20}+\frac{20}{20}i=\frac{-3}{2}+i.$$

En este caso tenemos dos elecciones para el cociente igual de buenas, tomamos $q_2 = -1+i$ y calculamos el resto:

$$(1+8i) = (-1+i)(2-4i)+(-1+2i).$$

Por ende, $r_2 = -1+2i$ observamos que $N(r_2) = 5$ y $N(r_1) = 20$, luego la división es correcta. Iteramos el proceso y tenemos que

$$z_2 = \frac{2-4i}{-1+2i} = -2,$$

luego $q_3 = -2$ y $r_3 = 0$. Como un máximo común divisor de α y β es el último resto no nulo, es decir $-1+2i$.

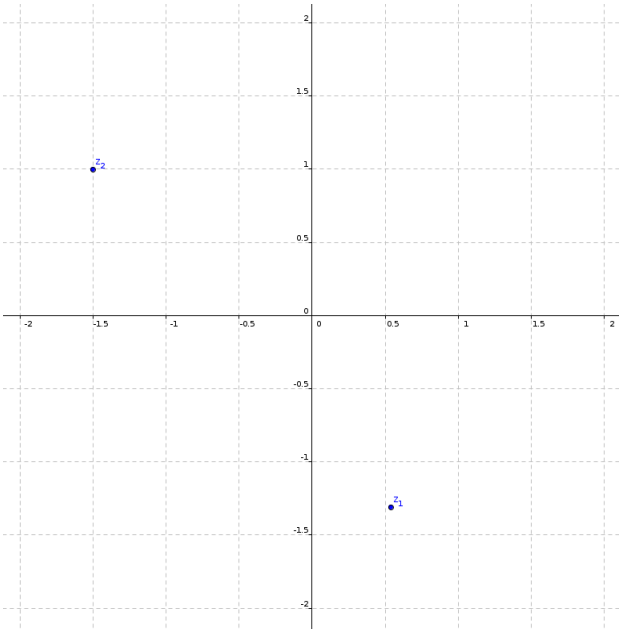


Figura II.1: Representación gráfica de los complejos z_1 y z_2

Observamos que si hubiéramos realizado otra elección de cociente $\widetilde{q}_2 = -2+i$ en la segunda división del algoritmo habríamos obtenido que

$$(1+8i) = (-2+i)(2-4i)+(1-2i).$$

Por lo tanto, $\widetilde{r}_2 = 1-2i$ e iterando $\widetilde{q}_3 = 2$ y $\widetilde{r}_3 = 0$. En otras palabras, el máximo común divisor obtenido en esta situación sería $1-2i$. Sin embargo, esto no contradice los resultados previos, porque sabemos que el máximo común divisor es único salvo asociados, es decir, salvo producto por unidades $U(\mathbb{Z}[i]) = \{1,-1,i,-i\}$. Dicho de otra manera, dependiendo de la elección (de las cuatro posibles) que hagamos en cada uno de los pasos del algoritmo podemos obtener diferentes valores, en este ejemplo, podríamos haber obtenido $-1+2i$, $1-2i$, $2+i$, $-2-i$. ¿Cómo están situados estos valores en el plano complejo?¿Qué elección de cocientes deberíamos hacer para obtener los últimos dos valores?

Una ligera modificación del algoritmo, nos permite obtener elementos s,t del dominio, de modo que se satisface la **Identidad de Bézout** (ver Proposición II.5.28), es decir, tales que $d = as+bt$.

ALGORITMO DE EUCLIDES EXTENDIDO

Entrada: Elementos a y b pertenecientes a un dominio euclídeo.

Salida: Un máximo común divisor d de a y b y elementos s,t del dominio tales que $d = as+bt$.

1. $r_0 := a$, $r_1 := b$, $s_0 := 1$, $t_0 := 0$, $s_1 := 0$, $t_1 := 1$.

2. $i \leftarrow 1$.

3. Mientras $r_i \neq 0$ hacer:

3.1. Aplicar (D.E.II) a r_{i-1} y r_i para obtener q_i, r_{i+1} con $r_{i-1} = r_i q_i + r_{i+1}$.

3.2. $s_{i+1} := s_{i-1} - q_i s_i$.

3.3. $t_{i+1} := t_{i-1} - q_i t_i$.

3.4. $i \leftarrow i+1$.

4. La salida es: r_{i-1} que es un máximo común divisor de a y b que se escribe como $r_{i-1} = a s_{i-1} + b t_{i-1}$.

Ejemplo II.5.37 En $(\mathbb{Z}/2\mathbb{Z})[x]$ queremos Calcular un m.c.d. y los elementos correspondientes de la igualdad de Bezout de $A(x) = x^6+x^5+x^3+x+1$ y $B(x) = x^4+x^3+x+1$.
En este caso, de acuerdo con la notación que del algoritmo de euclides $r_0 := A(x)$, $r_1 := B(x)$, $s_0 := 1$, $t_0 := 0$, $s_1 := 0$, $t_1 := 1$. Operando del mismo modo que en el EjemploA.2.16 obtenemos la siguiente lista de igualdades:

$$
\begin{aligned}
(r_0 = r_0s_0 + r_1t_0) \quad & x^6+x^5+x^3+x+1 = (x^6+x^5+x^3+x+1)\cdot(1) + (x^4+x^3+x+1)\cdot(0),\\
(r_1 = r_0s_1 + r_1t_1) \quad & x^4+x^3+x+1 = (x^6+x^5+x^3+x+1)\cdot(0) + (x^4+x^3+x+1)\cdot(1),\\
(r_2 = r_0s_2 + r_1t_2) \quad & x^2+x+1 = (x^6+x^5+x^3+x+1)\cdot(1) + (x^4+x^3+x+1)\cdot(x^2),\\
(r_3 = r_0s_3 + r_1t_3) \quad & 0 = (x^6+x^5+x^3+x+1)\cdot(x^2+1) + (x^4+x^3+x+1)\cdot(x^4+x^2+1).
\end{aligned}
$$

En consecuencia, $D(x) = x^2+x+1$, $S(x) = 1$ y $T(x) = x^2$.

Nota: Considerando las operaciones entre los coeficientes de los polinominos en $\mathbb{Z}/2\mathbb{Z} = \{0,1\}$, las divisiones entre polinominios en $(\mathbb{Z}/2\mathbb{Z})[x]$ para obtener los cocientes $q_1 = x^2$ y $q_2 = x^2+1$ se pueden realizar empleando el algoritmo habitual de la división entre polinomios.

Ejemplo II.5.38 Escribiendo el algoritmo para el Ejemplo II.5.36 de $\mathbb{Z}[i]$, es decir, si queremos obtener la identidad de Bézout para α y β:

$$
\begin{aligned}
11+3i &= (11+3i)\cdot(1) + (1+8i)\cdot(0),\\
1+8i &= (11+3i)\cdot(0) + (1+8i)\cdot(1),\\
2-4i &= (11+3i)\cdot(1) + (1+8i)\cdot(-1+i),\\
-1+2i &= (11+3i)\cdot(1-i) + (1+8i)\cdot(1+2i),\\
0 &= (11+3i)\cdot(*) + (1+8i)\cdot(*).
\end{aligned}
$$

La penúltima ecuación nos da la identidad de Bézout.

Ejercicio II.5.39 Dado un dominio de integridad D probar que la relación definida para todos $a,b \in D\backslash\{0\}$ por: aRb si y sólo si a y b son asociados, es una relación de equivalencia en $D\backslash\{0\}$.

Ejercicio II.5.40 Dado D un dominio de integridad. Probar que:

$$a \text{ y } b \text{ son son asociados si y sólo si } (a) = (b).$$

Ejercicio II.5.41 Supongamos que $a,b \in D$ con D dominio de integridad, $b \neq 0$ y $a \notin U(D)$. Demostrar que (ab) es un subconjunto propio de (b).

Ejercicio II.5.42 Dado $d \in \mathbb{N}_{\geq 1}$ consideramos los subanillos de $\mathbb{C}$ dados por

$$\mathbb{Z}[i\sqrt{d}] = \{a + bi\sqrt{d} : a,b \in \mathbb{Z}\}.$$

(Para $d = 1$, tenemos los Enteros de Gauss).
Desde cualquiera de estos subanillos, definimos la función $N : \mathbb{Z}[i\sqrt{d}] \to \mathbb{N}$ que a cada elemento de $\mathbb{Z}[i\sqrt{d}]$ lo envía en su módulo complejo al cuadrado, es decir,

$$N(a + b\sqrt{d}i) = a^2 + b^2 d.$$

Probar que N tiene las siguientes propiedades:

(I) $N(\alpha) = 0$ si y sólo si $\alpha = 0$.

(II) $N(\alpha\beta) = N(\alpha)N(\beta)$.

(III) $u \in U(\mathbb{Z}[i\sqrt{d}])$ si y sólo si $N(u) = 1$.

(IV) Si $N(\alpha)$ es primo, entonces α es irreducible.

Dar un ejemplo que pruebe que el recíproco de (IV) no se satisface.

Ejercicio II.5.43 Dado $d \in \mathbb{N}_{\geq 1}$ de modo que d no es cuadrado ($d \neq k^2$ para todo $k \in \mathbb{N}_{\geq 1}$), probar que el subanillo

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a,b \in \mathbb{Z}\} \subseteq \mathbb{R}$$

con la aplicación $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ dada por

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

satisface las propiedades:

(I) $N(\alpha) = 0$ si y sólo si $\alpha = 0$.

(II) $N(\alpha\beta) = N(\alpha)N(\beta)$.

(III) $u \in U(\mathbb{Z}[\sqrt{d}])$ si y sólo si $N(u) = \pm 1$.

(IV) Si $N(\alpha)$ es primo, entonces α es irreducible.

Dar un ejemplo que pruebe que el recíproco de (IV) no se satisface.

Ejercicio II.5.44 Un entero d se dice que es un cuadrado si existe $k \in \mathbb{Z}$ tal que $d = k^2$. Un entero d se dice que es **libre de cuadrados** si no existe un número primo p tal que p^2 divide a d. Dado $d \in \mathbb{N}_{\geq 1}$, probar que:

(I) Si d es libre de cuadrados entonces d no es un cuadrado.

(II) Si d es un cuadrado, entonces $\mathbb{Z}[\sqrt{d}] = \mathbb{Z}$ y si d no es un cuadrado entonces existe c libre de cuadrados tal que $\mathbb{Z}[\sqrt{d}]$ es un subanillo propio $\mathbb{Z}[\sqrt{c}]$.

(III) Si d es un cuadrado, entonces $\mathbb{Z}[i\sqrt{d}]$ es un subanillo propio de $\mathbb{Z}[i]$ y si d no es un cuadrado entonces existe c libre de cuadrados tal que $\mathbb{Z}[i\sqrt{d}]$ es un subanillo propio $\mathbb{Z}[i\sqrt{c}]$.

Dar un ejemplo que ilustre cada uno de los casos anteriores.

Ejercicio II.5.45 Probar que si $d \in \mathbb{Z}$ es un entero libre de cuadrados (Ver Ejercicio II.5.44) y $d > 2$. Probar que:

(I) Las unidades de $\mathbb{Z}[i\sqrt{d}]$ son 1 y -1.

(II) 2 es irreducible en $\mathbb{Z}[i\sqrt{d}]$.

(III) $\pm i\sqrt{d}$ es irreducible en $\mathbb{Z}[i\sqrt{d}]$.

(IV) $1 \pm i\sqrt{d}$ es irreducible en $\mathbb{Z}[i\sqrt{d}]$.

(V) $\mathbb{Z}[i\sqrt{d}]$ no es un D.F.U.

Ejercicio II.5.46 Determinar si $\mathbb{Z}[\sqrt{10}]$ es o no un D.F.U.

Ejercicio II.5.47 Dado D un dominio y $a \in D$ ¿Cuál es un máximo común divisor de a y 0_D? ¿y de 0_D y 0_D? ¿Cuál es un mínimo común múltiplo de a y 0_D? ¿y de 0_D y 0_D?

Ejercicio II.5.48 Dado D un dominio, $x \in D$ y $u \in U(D)$ ¿Cuál es un máximo común divisor de x y u? ¿Cuál es un mínimo común múltiplo de x y u?

Ejercicio II.5.49 Sea D un D.I.P. Demostrar que todo ideal propio (no nulo y distinto del total) está contenido en un ideal maximal de D.

Ejercicio II.5.50 Sea D un D.I.P. y $a, b, d, m \in D$. Entonces se cumple que:

(I) $(a) + (b) = (d)$ si y sólo si d es un máximo común divisor de a y b.
(*Identidad de Bezout*)

(II) $(a) \cap (b) = (m)$ si y sólo si m es un mínimo común múltiplo de a y b.

Nota: De acuerdo con la Proposición II.2.11 y la Observación II.2.9 se tiene que $(a)+(b) = ((a) \cup (b)) = (a,b)$.

Ejercicio II.5.51 En general, la identidad de Bezout no es cierta en un D.F.U. que no son D.I.P. ¿Podrías dar un ejemplo de dos elementos a y b de un D.F.U. que no verifiquen la Identidad de Bezout?

Ejercicio II.5.52 $\mathbb{Z}[i]$ es un dominio euclídeo respecto a la función $N(a+bi) = a^2 + b^2$

Ejercicio II.5.53 Sea (D, δ) un dominio euclideo. Probar que u es unidad en D si y sólo si $\delta(u) = \delta(1_D)$.

Ejercicio II.5.54 Sea (D,δ) un dominio euclideo. Demostrar que si a y b son asociados en D entonces $\delta(a)=\delta(b)$. ¿Es el recíproco cierto?

Ejercicio II.5.55 Dado (D,δ) un dominio euclídeo. Probar que q,r en (DE.II) son únicos si y sólo si $\delta(a+b)\leq \text{máx}(\delta(a),\delta(b))$.
(Para más información leer [13])

Ejercicio II.5.56 Dado D un dominio que cumple la condición (DE.II) para una función $\delta: D\backslash\{0_D\}\to\mathbb{N}$. Probar que existe una función $\nu: D\backslash\{0_D\}\to\mathbb{N}$ verificando (DE.I) y (DE.II).

Ejercicio II.5.57 Emplear el algoritmo de Euclides para calcular un máximo común divisor en $\mathbb{Z}$ de $a=253872$ y $b=886$.

Ejercicio II.5.58 Emplear el algoritmo de Euclides para calcular un máximo común divisor en $\mathbb{Q}[x]$ de $P(x)=x^6+3x^5+2x^4+7x^3+3x^2+2x+6$ y $Q(x)=x^3+4x^2+5x+6$.

Ejercicio II.5.59 Emplear el algoritmo de Euclides para calcular un máximo común divisor en $\mathbb{Z}[i]$ de $\alpha=427+32i$ y $\beta=16+81i$.

II.6 Anillos de polinomios

II.6.1 Construcción del anillo de polinomios. Grado de un polinomio

Una fuente de ejemplos habitual en la teoría de anillos son los **anillos de polinomios**. En gran parte de los textos elementales, se definen los polinomios con coeficientes en R como **sumas finitas de monomios** donde los monomios son expresiones de la forma: ax^n, con $a \in R$ y $n \in \mathbb{N}$. En esta subsección, veremos como definir formalmente el conjunto de polinomios con coeficientes en un anillo a partir de las nociones básicas de teoría de conjuntos y probaremos que este conjunto se puede dotar de estructura de anillo.

*Nota (Sucesiones): Una **sucesión de elementos de un conjunto** X, no vacío, es una aplicación $f : \mathbb{N} \to X$, donde $\mathbb{N} = \{0,1,2,\dots\}$. Habitualmente, las sucesiones no se representan mediante la notación funcional. Para representar una sucesión empleamos los elementos del conjunto imagen. De este modo, si para todo $j \in \mathbb{N}$ denotamos por $x_j := f(j)$, la sucesión f se representa por $(x_j)_{j=0}^{\infty}$ y cada x_j se denomina término.*
El conjunto de todas las sucesiones de un conjunto X, es decir, el conjunto de todas las aplicaciones de $\mathbb{N}$ en X se denota por $X^{\mathbb{N}}$.

Definición II.6.1 (Anillo de polinomios) Dado $(R,+,\cdot)$ un anillo, un **polinomio con coeficientes en** R es un elemento $(a_j)_{j=0}^{\infty} \in R^{\mathbb{N}}$ tal que existe $n \in \mathbb{N}$ de modo que $a_j = 0$ si $j > n$, es decir, formalmente un polinomio es una **sucesión de elementos del anillo cuyos términos son nulos de un lugar en adelante**.
Tradicionalmente, no se emplea la notación sucesional y un polinomio

$$(a_j)_{j=0}^{\infty} = (a_0, a_1, \dots, a_{n-1}, a_n, 0, 0, 0, \dots)$$

cuyos términos son nulos para todo $j > n$, se denota mediante

$$\sum_{j=0}^{n} a_j x^j \quad \text{o} \quad a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n.$$

El conjunto de todos los polinomios con coeficientes en R se denota por $R[x]$. Sobre este conjunto se definen la suma y el producto del modo usual operaciones:

$$\begin{array}{rcl} + : R[x] \times R[x] & \longrightarrow & R[x] \\ \left((a_j)_{j=0}^{\infty}, (b_j)_{j=0}^{\infty}\right) & \longrightarrow & (a_j + b_j)_{j=0}^{\infty} \end{array} \qquad \begin{array}{rcl} \cdot : R[x] \times R[x] & \longrightarrow & R[x] \\ \left((a_j)_{j=0}^{\infty}, (b_j)_{j=0}^{\infty}\right) & \longrightarrow & (c_j)_{j=0}^{\infty} \end{array}$$

donde $c_j := \sum_{k=0}^{j} a_k b_{j-k}$ (Como $(R,+)$ es abeliano $c_j = \sum_{k=0}^{j} a_{j-k} b_k$).

Proposición II.6.2 Sea $(R,+,\cdot)$ un anillo. Entonces, se tiene que $(R[x],+,\cdot)$ es un anillo.

Demostración. Como R es un anillo es no vacío y por lo tanto $R[x]$ es **no vacío**.

Las operaciones definidas sobre $R[x]$ son **operaciones internas**: dados dos polinomios $P(x) = \sum_{j=0}^{n} a_j x^j$ y $Q(x) = \sum_{j=0}^{m} b_j x^j$, los términos $a_j + b_j$ de la suma $P(x) + Q(x)$ son nulos para todo $j > \max(m,n)$ y los términos c_j del producto $P(x) \cdot Q(x)$ son nulos para todo $j > n+m$ porque en todos los sumandos de la definición de c_j al menos uno de los factores es nulo. Por consiguiente, $P(x) + Q(x)$ y $P(x) \cdot Q(x)$ son polinomios.

Veamos que $(R[x],+)$ es un **grupo abeliano**, es decir, que se satisface (R.I). Dado que $(R,+,\cdot)$ es un anillo, tenemos que $(R,+)$ es un grupo abeliano. Las propiedades asociativa y conmutativa de $(R[x],+)$ se obtienen empleando las propiedades correspondientes de $(R,+)$.

Del mismo modo, se comprueba de forma directa que el polinomio con todos los coeficientes nulos, el polinomio nulo, $(0,0,0,\dots)$ es elemento neutro de la suma y que el inverso para la suma de un polinomio $\sum_{j=0}^{n} a_j x^j$ es $\sum_{j=0}^{n}(-a_j)x^j$.

Veamos que $(R[x],\bullet)$ es **semigrupo**, es decir, que se satisface (R.II). Dados tres polinomios: $P_1(x)=\sum_{j=0}^{n_1} a_{1,j}x^j$, $P_2(x)=\sum_{j=0}^{n_2} a_{2,j}x^j$ y $P_3(x)=\sum_{j=0}^{n_3} a_{3,j}x^j$. Veamos que el coeficiente $j-$ésimo de $P_1(x)(P_2(x)P_3(x))$ coincide con el coeficiente $j-$ésimo de $(P_1(x)P_2(x))P_3(x)$. Empleando que las propiedades (R.I), (R.II) y (R.III) que tiene R por ser anillo, si $P_1(x)P_2(x)=\sum_{j=0}^{n_1+n_2} b_j x^j$ y $P_2(x)P_3(x)=\sum_{j=0}^{n_2+n_3} d_j x^j$, se tiene que:

$$\begin{aligned}\sum_{k=0}^{j} a_{1,k}\cdot d_{j-k} &= \sum_{k=0}^{j} a_{1,k}\cdot\left(\sum_{m=0}^{j-k} a_{2,(j-k)-m}\cdot a_{3,m}\right)=\sum_{k=0}^{j}\left(\sum_{m=0}^{j-k} a_{1,k}\cdot a_{2,(j-k)-m}\cdot a_{3,m}\right)\\ &=\sum_{m=0}^{j}\left(\sum_{k=0}^{j-m} a_{1,k}\cdot a_{2,(j-k)-m}\cdot a_{3,m}\right)=\sum_{m=0}^{j}\left(\sum_{k=0}^{j-m} a_{1,k}\cdot a_{2,(j-m)-k}\right)\cdot a_{3,m}=\sum_{m=0}^{j} b_{j-m}\cdot a_{3,m}.\end{aligned}$$

Veamos que se verifica la **propiedad distributiva** polinomios (R.III). Con la notación de la prueba de (R.II), dados $P_1(x),P_2(x),P_3(x)$ polinomios de $R[x]$. Veamos que el coeficiente $j-$ésimo de $P_1(x)(P_2(x)+P_3(x))$ coincide con el coeficiente $j-$ésimo de $P_1(x)P_2(x)+P_1(x)P_3(x)$. Como R es un anillo, vemos que:

$$\sum_{k=0}^{j} a_{1,k}\cdot(a_{2,j-k}+a_{3,j-k})=\sum_{k=0}^{j}(a_{1,k}\cdot a_{2,j-k}+a_{1,k}a_{3,j-k})=\sum_{k=0}^{j} a_{1,k}\cdot a_{2,j-k}+\sum_{k=0}^{j} a_{1,k}a_{3,j-k}.$$

Análogamente, se prueba que $(P_2(x)+P_3(x))P_1(x)=P_2(x)P_1(x)+P_2(x)P_1(x)$. ■

Proposición II.6.3 Sea $(R,+,\cdot)$ un anillo conmutativo. Entonces $(R[x],+,\cdot)$ es un anillo conmutativo.

Demostración. Dados dos polinomios $P(x)=\sum_{j=0}^{n} a_j x^j$ y $Q(x)=\sum_{j=0}^{m} b_j x^j$ el coeficiente $j-$ésimo de $P(x)Q(x)$ es $\sum_{k=0}^{j} a_k b_{j-k}$ y el coeficiente $j-$ésimo de $Q(x)P(x)$ es $\sum_{k=0}^{j} b_k a_{j-k}$, como R es conmutativo ambas expresiones coinciden. Por tanto, $P(x)Q(x)=Q(x)P(x)$ ■

Proposición II.6.4 Sea $(R,+,\cdot)$ un anillo unitario. Entonces $(R[x],+,\cdot)$ es un anillo unitario.

Demostración. Veamos que el polinomio $N(x)=1$, es decir, el polinomio con $a_0=1_R$ y $a_n=0$ si $n\in\mathbb{N}_{\geq 1}$, es el polinomio neutro para el producto.
Dado $Q(x)=\sum_{j=0}^{m} b_j x^j$ un polinomio de $R[x]$, tenemos que el coeficiente $j-$ésimo de $N(x)Q(x)$ es $c_j=\sum_{k=0}^{j} a_k b_{j-k}=a_0 b_j=b_j$ y el coeficiente $j-$ésimo de $Q(x)N(x)$ es $c_j=\sum_{k=0}^{j} b_k a_{j-k}=b_j a_0=b_j$. Por consiguiente, $N(x)Q(x)=Q(x)N(x)=Q(x)$ y $N(x)$ es el elemento neutro del producto. ■

Ejemplos II.6.5 (1) Como $(\mathbb{Z},+,\cdot)$, $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ son anillos conmutativos y unitarios, los correspondientes anillos de polinomios $(\mathbb{Z}[x],+,\cdot)$, $(\mathbb{Z}/n\mathbb{Z}[x],+,\cdot)$, $(\mathbb{Q}[x],+,\cdot)$ $(\mathbb{R}[x],+,\cdot)$, $(\mathbb{C}[x],+,\cdot)$ son también anillos conmutativos y unitarios.

(2) El conjunto de polinomios $((3\mathbb{Z})[x],+,\cdot)$, cuyos coeficientes son múltiplos de 3, es un anillo conmutativo pero no es unitario.

(3) El conjunto de polinomios $(\mathrm{Mat}_{n\times n}(\mathbb{Q})[x],+,\cdot)$, cuyos coeficientes son matrices con coeficientes racionales, es un anillo unitario pero no es conmutativo.

Observación II.6.6 Empleando los resultados anteriores, podemos definir el anillo de polinominos en **varias variables** de forma recursiva. De este modo, si $(R,+,\cdot)$ es un anillo, por la Proposición II.6.2, tenemos que $(R[x],+,\cdot)$ es un anillo y podemos considerar $R[x,y] := (R[x])[y]$ que de nuevo por la Proposición II.6.2 sabemos que es un anillo.

Iterando el proceso, podemos definir $R[x_1,x_2,\ldots,x_m] := (R[x_1,x_2,\ldots,x_{m-1}])[x_m]$ el anillo de polinomios para m variables. Observamos que si R es unitario, entonces estos anillos son unitarios, ver Proposición II.6.3, y si R es conmutativo, estos anillos son conmutativos ver Proposición II.6.4.

Cabe destacar que también es posible definir el conjunto de polinomios en m variables con coeficientes en R de forma directa definiendo un polinomio como una aplicación de $\mathbb{N}^m$ en R, $A : \mathbb{N}\times\cdots(m \text{ veces})\cdots\times\mathbb{N}\to R$, de forma que existe $n\in\mathbb{N}$ tal que $A(j_1,\ldots,j_m) = 0_R$ si $|j| = j_1+j_2+\cdots+j_m > n$. Definiendo las operaciones de manera natural sobre este conjunto, se trata de un ejercicio demostrar que ambas definiciones conducen a anillos isomorfos.

En el estudio de los anillos de polinomios es fundamental la noción del grado.

Definición II.6.7 Sea $(R,+,\cdot)$ un anillo y $P\in R[x]\backslash\{0\}$ un polinomio con coeficientes $(a_j)_{j=0}^{\infty}\in R^{\mathbb{N}}$, que por definición son nulos de un lugar en adelante. Entonces, se define el **grado de** $P(x)$ por

$$\operatorname{gr}(P(x)) := \operatorname{máx}\{j\in\mathbb{N} : a_j\neq 0\}.$$

En otras palabras, el **grado de** $P(x)$ es $n\in\mathbb{N}$ si y solamente si

$$P(x) = \sum_{j=0}^{n} a_j x^j = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n \qquad \text{con} \quad a_n \neq 0.$$

Proposición II.6.8 — Grado de la suma de dos polinomios. Sean $(R,+,\cdot)$ un anillo y $P(x),Q(x)\in R[x]\backslash\{0\}$ dos polinomios con $P(x)+Q(x)\neq 0$. Entonces se cumple que:

(I) Si $\operatorname{gr}(P(x))\neq\operatorname{gr}(Q(x))$, entonces $\operatorname{gr}(P(x)+Q(x)) = \operatorname{máx}(\operatorname{gr}(P(x)),\operatorname{gr}(Q(x)))$.

(II) $\operatorname{gr}(P(x)+Q(x))\leq\operatorname{máx}(\operatorname{gr}(P(x)),\operatorname{gr}(Q(x)))$.

Demostración. Consideramos dos polinomios $P(x)=\sum_{j=0}^{n}a_jx^j$ y $Q(x)=\sum_{j=0}^{m}b_jx^j$ con $a_n\neq 0$ y con $b_m\neq 0$, es decir, con $\operatorname{gr}(P(x))=n$ y con $\operatorname{gr}(Q(x))=m$. Sin pérdida de generalidad, podemos suponer que $m\leq n$, es decir que $n=\operatorname{máx}(\operatorname{gr}(P(x)),\operatorname{gr}(Q(x)))$. En este caso, podemos escribir $P(x)+Q(x)=\sum_{j=0}^{n}(a_j+b_j)x^j$.
Si $m<n$, $a_n+b_n=a_n\neq 0$, luego $\operatorname{gr}(P(x)+Q(x))=n$ y se verifica (I).
Si $n=m$ y $a_n+b_n\neq 0$, se tiene que $\operatorname{gr}(P(x)+Q(x))=n$.
Si $n=m$ y $a_n+b_n=0$, se tiene que $\operatorname{gr}(P(x)+Q(x))<n$.
Reuniendo toda la información, concluimos que se verifica (II). ■

Proposición II.6.9 — Grado del producto de dos polinomios. Sean $(R,+,\cdot)$ un anillo conmutativo y $P(x),Q(x)\in R[x]\backslash\{0\}$ dos polinomios con $P(x)Q(x)\neq 0$. Entonces se cumple que:

$$\operatorname{gr}(P(x)Q(x))\leq\operatorname{gr}(P(x))+\operatorname{gr}(Q(x)).$$

Demostración. Consideramos dos polinomios $P(x)=\sum_{j=0}^{n}a_jx^j$ y $Q(x)=\sum_{j=0}^{m}b_jx^j$ con $a_n\neq 0$ y con $b_m\neq 0$, es decir, con $\mathrm{gr}(P(x))=n$ y con $\mathrm{gr}(Q(x))=m$. Los términos c_j del producto $P(x)\cdot Q(x)$ son nulos para todo $j>n+m$ porque en todos los sumandos de la definición de esos c_j al menos uno de los factores es nulo, entonces

$$P(x)\cdot Q(x)=\sum_{j=0}^{n+m}(\sum_{k=0}^{j}a_kb_{j-k})x^j=\sum_{j=0}^{n+m-1}(\sum_{k=0}^{j}a_kb_{j-k})x^j+a_nb_mx^{n+m}.$$

Por consiguiente, si $a_nb_m=0$ tenemos que $\mathrm{gr}(P(x)Q(x))<n+m$ y si $a_nb_m\neq 0$ tenemos que $\mathrm{gr}(P(x)Q(x))=n+m$, en ambos casos se satisface la desigualdad. ■

La desigualdad de la proposición anterior puede ser estricta como muestra el siguiente ejemplo.

Ejemplo II.6.10 Consideramos los polinomios $P(x)=2x+1$ y $Q(x)=3x+1$ en $(\mathbb{Z}/6\mathbb{Z})[x]$. Observamos que $P(x)Q(x)=5x+1$, luego

$$\mathrm{gr}(P(x)Q(x))=1<1+1=\mathrm{gr}(P(x))+\mathrm{gr}(Q(x)).$$

II.6.2 Homomorfismo de evaluación. Raíz de un polinomio

El siguiente resultado nos permite, abusando de la notación, considerar el anillo R como un subanillo de $R[x]$ de forma natural.

Proposición II.6.11 Sea $(R,+,\cdot)$ un anillo. Entonces R es isomorfo a un subanillo de $R[x]$.

Demostración. Consideramos la aplicación $\psi:R\to R[x]$ que a cada elemento $a\in R$ lo envía en el polinomio $P(x)$ con $a_0=a$ y $a_j=0$ si $j\in\mathbb{N}_{\geq 1}$, es decir, $\psi(a)=(a,0,0,\dots)$. Por como se definen la suma y el producto de polinomios, podemos afirmar que ψ es un homomorfismo de anillos. Si $\psi(a)=\psi(b)$, entonces tenemos que todos los coeficientes de los polinomios son iguales, luego $a=b$, es decir, ψ es inyectivo.
Finalmente, sabemos, por las Propiedades II.3.3, que $\mathrm{Im}\psi$ es subanillo de $R[x]$ y, por el Primer Teorema de Isomorfía, concluimos que $R\approx\mathrm{Im}\psi$. ■

Tenemos la siguiente relación entre la característica de R y la característica de $R[x]$.

Proposición II.6.12 Sea R un anillo unitario. Entonces se cumple que $\mathrm{car}(R[x])=\mathrm{car}(R)$.

Demostración. Recordamos que el elemento neutro del producto en $R[x]$ es el polinomio con todos los coeficientes nulos excepto el primo que es 1_R, es decir, $a_j=0$ si $j\in\mathbb{N}_{\geq 1}$ y $a_0=1$, ver Proposición II.6.3. Por la definición de la suma de polinomios en $R[x]$, se tiene que dado $n\in\mathbb{N}_{\geq 1}$ observamos que $n1_R=0_R$ si y solo si $n1_{R[x]}=0_{R[x]}$. Luego $O(1_R)=O(1_{R[x]})$ y, por el Teorema II.2.16, concluimos que $\mathrm{car}(R[x])=\mathrm{car}(R)$. ■

Ejemplos II.6.13 Por la proposición anterior tenemos que $\mathrm{car}(\mathbb{Z}[x])=\mathrm{car}(\mathbb{Z})=0$, que $\mathrm{car}(\mathbb{Q}[x])=\mathrm{car}(\mathbb{Q})=0$, que $\mathrm{car}(\mathbb{R}[x])=\mathrm{car}(\mathbb{R})=0$ y que $\mathrm{car}(\mathbb{C}[x])=\mathrm{car}(\mathbb{C})=0$.
Por otro lado, se cumple que que $\mathrm{car}(\mathbb{Z}/n\mathbb{Z}[x])=\mathrm{car}(\mathbb{Z}/n\mathbb{Z})=n\in\mathbb{N}_{\geq 1}$.

Para poder definir la noción de evaluación y la noción de raíz de un modo sencillo, restringiremos nuestro estudio a anillos conmutativos y unitarios.

Teorema II.6.14 (Extensión de un homomorfismo). Sean R y S dos anillos conmutativos y unitarios y $f : R \to S$ un homomorfismo de anillos unitarios. Para cada $s \in S$ consideramos la aplicación

$$\begin{array}{rccc} f_s: & R[x] & \longrightarrow & S \\ & \sum_{j=0}^{n} a_j x^j & \longrightarrow & \sum_{j=0}^{n} f(a_j) s^j \end{array}$$

que se denomina la **extensión de f mediante la evaluación en s**. Entonces se cumple que:

(I) para cada $a \in R$ se tiene que $f_s(a) = f(a)$ y que $f_s(x) = s$.

(II) f_s es un homomorfismo de anillos.

(III) f_s es la única aplicación que satisface (I) y (II).

Demostración. (I) Directo de la definición de f_s.

(II) Dados dos polinomios $P(x) = \sum_{j=0}^{n} a_j x^j$ y $Q(x) = \sum_{j=0}^{m} b_j x^j$, veamos que f_s es homomorfismo de anillos, es decir, que satisface (HA.I) y (HA.II). Sin pérdida de generalidad, suponemos que $n \geq m$, empleando la definición de f_s, que f satisface (HA.I) y que $(S,+,\cdot)$ es un anillo, vemos que

$$f_s(P(x)+Q(x)) = f_s\Big(\sum_{j=0}^{n}(a_j+b_j)x^j\Big) \overset{\text{def.}}{=} \sum_{j=0}^{n} f(a_j+b_j)s^j \overset{\text{(HA.I)}}{=} \sum_{j=0}^{n}\Big(f(a_j)+f(b_j)\Big)s^j$$

$$\overset{\substack{(S,+)\text{ Conmut.}\\ (S,+,\cdot)\text{ Distr.}}}{=} \sum_{j=0}^{n}\Big(f(a_j)\Big)s^j + \sum_{j=0}^{n}\Big(f(b_j)\Big)s^j \overset{\substack{b_j=0\\ \text{si } j>m}}{=} \sum_{j=0}^{n}\Big(f(a_j)\Big)s^j + \sum_{j=0}^{m}\Big(f(b_j)\Big)s^j = f_s(P(x)) + f_s(Q(x)).$$

Por tanto, f_s satisface (HA.I).

Recordamos que los coeficientes del producto de los polinomios $P(x)Q(x)$ se definen como $c_j = \sum_{k=0}^{j} a_k b_{j-k}$. Dado que f es un homomorfismo de anillos y que $(S,+,\cdot)$ es un anillo conmutativo, observamos que

$$f_s(P(x)Q(x)) = f_s\Big(\sum_{j=0}^{n+m} c_j x^j\Big) \overset{\text{def.}}{=} \sum_{j=0}^{n+m} f(c_j)s^j = \sum_{j=0}^{n+m} f\Big(\sum_{k=0}^{j} a_k b_{j-k}\Big)s^j \overset{\text{(HA.I)}}{=} \sum_{j=0}^{n+m}\Big(\sum_{k=0}^{j} f(a_k b_{j-k})\Big)s^j$$

$$\overset{\text{(HA.II)}}{=} \sum_{j=0}^{n+m}\Big(\sum_{k=0}^{j} f(a_k)f(b_{j-k})\Big)s^j \overset{\substack{(S,\bullet)\\ \text{Conmut.}}}{=} \sum_{j=0}^{n+m}\sum_{k=0}^{j} f(a_k)s^k f(b_{j-k})s^{k-j} \overset{\substack{(S,+)\\ \text{Conmut.}}}{=} \sum_{k=0}^{n+m}\sum_{j=k}^{n+m} f(a_k)s^k f(b_{j-k})s^{k-j}$$

$$\overset{\text{Distr.}}{=} \sum_{k=0}^{n+m} f(a_k)s^k\Big(\sum_{j=k}^{n+m} f(b_{j-k})s^{k-j}\Big) \overset{\ell=j-k}{=} \sum_{k=0}^{n+m} f(a_k)s^k\Big(\sum_{\ell=0}^{n+m-k} f(b_\ell)s^\ell\Big)$$

$$\overset{\substack{a_k=0,\,k>n\\ b_\ell=0,\,\ell>m}}{=} \sum_{k=0}^{n} f(a_k)s^k\Big(\sum_{\ell=0}^{m} f(b_\ell)s^\ell\Big) \overset{\text{Distr.}}{=} \Big(\sum_{k=0}^{n}\Big(f(a_k)\Big)s^k\Big)\Big(\sum_{\ell=0}^{m}\Big(f(b_\ell)\Big)s^\ell\Big) = f_s(P(x))f_s(Q(x)).$$

En consecuencia, f_s satisface (HA.II) y concluimos que f_s es un homomorfismo de anillos.

(III) Si existe otra aplicación g satisface (I) y (II), dado $P(x) = \sum_{j=0}^{n} a_j x^j$ tenemos que

$$g(P(x)) = g\Big(\sum_{j=0}^{n} a_j x^j\Big) \overset{\text{(HA.I)}}{=} \sum_{j=0}^{n} g(a_j x^j) \overset{\text{(HA.II)}}{=} \sum_{j=0}^{n} g(a_j)(g(x))^j \overset{\text{(I)}}{=} \sum_{j=0}^{n} f(a_j)s^j \overset{\text{def.}}{=} f_s(P(x)). \quad \blacksquare$$

Observación II.6.15 Tenemos que f_s es también un homomorfismo de anillos unitarios, porque $f_s(1_R) = f(1_R) = 1_S$.

Habitualmente, el homomorfismo de extensión descrito en el Teorema II.6.14 se aplica a un anillo conmutativo S y un un subanillo suyo R tomando $f = i : R \to S$ la inclusión canónica.

Corolario II.6.16 (Homomorfismo de evaluación) Sea S un anillo conmutativo y unitario y R un subanillo de S con $1_S \in R$. Para cada elemento $s \in S$ consideramos la aplicación **evaluación en** s dada por

$$\begin{array}{rccc} e_s: & R[x] & \longrightarrow & S \\ & \displaystyle\sum_{j=0}^{n} a_j x^j & \longrightarrow & P(s) := \displaystyle\sum_{j=0}^{n} a_j s^j. \end{array}$$

Entonces se cumple que e_s es un homomorfismo de anillos.

Demostración. Basta aplicar el Teorema II.6.14 a la inclusión canónica $i : R \to S$ tenemos que la aplicación e_s coincide con el homomorfismo de anillos i_s. ■

Observación II.6.17 En particular, como todo anillo es subanillo de sí mismo, podemos aplicar el ejercicio anterior para $S = R$ y obtenemos $e_r : R[x] \to R$ con $r \in R$.
Si el anillo R **no es conmutativo**, dados $P(x), Q(x) \in R[x]$ puede ser que $e_r(P(x))e_r(Q(x)) \neq e_r(P(x)Q(x))$, es decir, puede que no sea lo mismo evaluar cada uno de los polinomios en r y después hacer el producto $e_r(P(x))e_r(Q(x))$ que hacer primero el producto de los polinomios y luego evaluar $e_r(P(x)Q(x))$.
Por ejemplo, si R es el anillo de los cuaterniones $\mathbb{H}$ (ver Ejercicio I.2.22, II.4.32) considerando los polinomios $P(x) = x + i$ y $Q(x) = x - i$ tenemos que $R(x) = P(x)Q(x) = x^2 + 1$, pero

$$\begin{aligned} e_j(P(x))e_j(Q(x)) = P(j)Q(j) = (j+i)(j-i) = j^2 + ij - ji - i^2 = -1 + k - (-k) - (-1) = 2k, \\ e_j(P(x)Q(x)) = R(j) = j^2 + 1 = -1 + 1 = 0. \end{aligned}$$

En este contexto, la idea intuitiva de raíz de un polinomio pierde el sentido clásico y, por este motivo, trabajar con polinomios con coeficientes en un anillo no conmutativo está fuera de los objetivos de este curso.

Definición II.6.18 Sea S un anillo conmutativo y unitario, $s \in S$, R un subanillo de S con $1_S \in R$ y $P(x) \in R[x]$. Decimos que s es una **raíz o cero de** $P(x)$ en S si $e_s(P(x)) = 0$, es decir, si $P(s) = 0$.

Proposición II.6.19 Sea S un anillo conmutativo y unitario, $s \in S$, R un subanillo de S con $1_S \in R$ y $P(x) \in R[x]$. Entonces el conjunto $\{P(x) \in R[x] : P(s) = 0\}$ de los polinomios de $R[x]$ que tienen a s como raíz es un ideal de $R[x]$.

Demostración. Observamos que el conjunto de todos los polinomios de $R[x]$ que tienen a s como raíz es

$$\{P(x) \in R[x] : P(s) = 0\} = \{P(x) \in R[x] : e_s(P(x)) = 0\} = \mathrm{Ker}(e_s).$$

Por el Corolario II.6.16, tenemos que $e_s : R[x] \to S$ es un homomorfismo de anillos y por las Propiedades II.3.3 sabemos que $\mathrm{Ker}(e_s)$ que es un ideal. ■

Proposición II.6.20 Sean S un anillo conmutativo y unitario, $s \in S$, R un subanillo de S con $1_S \in R$. Denotamos por $R[s] := \mathrm{Im}(e_s)$.
Entonces $R[s]$ es el menor subanillo de S que contiene a R y a s.

Demostración. Por las Propiedades II.3.3, sabemos que $R[s] := \mathrm{Im}(e_s)$ es un subanillo de S. Dado $r \in R$ considerando el polinomio $P(x) = r$ (constante igual a r) vemos que $e_s(P(x)) = r$, luego $r \in R[s]$ y concluimos que $R \subseteq R[s]$.
Del mismo modo, considerando el polinomio $P(x) = x$ vemos que $e_s(P(x)) = s$, luego $s \in R[s]$ y tenemos que $s \in R[s]$. En otras palabras, $R[s]$ es un subanillo de S que contiene a R y a s.

Veamos ahora que $R[s]$ es el subanillo más pequeño con esta propiedad. Si $T \subseteq S$ es un subanillo de S que contiene a R y a s, por ser subanillo, contiene a todas las potencias positivas de s ($s^j \in T$) y a los productos de las potencias por elementos de $a \in R$ ($as^j \in T$ para todo $j \in \mathbb{N}$). Por ser subanillo, también tiene que contener a las sumas de expresiones de este tipo. En consecuencia, contiene a todos los elementos de la forma $\sum_{j=0}^{n} a_j s^j$ con $a_j \in R$, entonces $R[s] \subseteq T$. ■

Nota: *Esta notación se ha empleado en secciones anteriores para definir ciertos anillos (Por ejemplo: $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{5}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{6}]$). Mediante la Proposición II.6.20, eligiendo adecuadamente R, S y $s \in S$ podemos construir anillos con la misma notación (Por ejemplo: tomando $R = \mathbb{Z}$, $S = \mathbb{C}$ y $s = i$ definimos $\mathbb{Z}[i]$). Se puede comprobar que los anillos $R[s]$, definidos de manera simultánea de este modo, coinciden con los anillos homónimos definidos anteriormente de manera particular, es decir, la notación es adecuada.*

El Teorema II.6.14 también se puede aplicar a otros homomorfismos como muestra el siguiente corolario.

Corolario II.6.21 Dados $n \in \mathbb{N}_{\geq 2}$, y dos polinomios $P(x), Q(x) \in \mathbb{Z}[x]$.
Entonces se obtiene el mismo resultado si, en primer lugar, se operan los polinomios en $\mathbb{Z}[x]$ y después el resultado se transforma en un polinomio de $(\mathbb{Z}/n\mathbb{Z})[x]$ considerando sus coeficientes módulo n o, en otro orden, si primero se transforman $P(x), Q(x)$ en polinomios de $(\mathbb{Z}/n\mathbb{Z})[x]$ considerando sus coeficientes módulo n y luego se operan en dicho anillo.

Demostración. Por las Propiedades II.3.6, la composición de $p : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ el homomorfismo sobreyectivo de paso al cociente con la inclusión canónica $\psi : \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})[x]$ dada en la Proposición II.6.11, define un homomorfismo de anillos, $f = (\psi \circ p) : \mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})[x]$. Aplicando el Teorema II.6.14, para $R = \mathbb{Z}$, $S = (\mathbb{Z}/n\mathbb{Z})[x]$ y $s = x \in (\mathbb{Z}/n\mathbb{Z})[x]$ tenemos que existe un homomorfismo de anillos

$$\begin{array}{rccc} f_x : & \mathbb{Z}[x] & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})[x] \\ & \displaystyle\sum_{j=0}^{n} a_j x^j & \longrightarrow & \displaystyle\sum_{j=0}^{n} f(a_j)x^j \qquad \text{con} \quad f(a_j) = [a_j]_n \end{array}$$

Por consiguiente, dados dos polinomios $P(x), Q(x) \in \mathbb{Z}[x]$, como f_x es homomorfismo, se cumple que

$$f_x(P(x) + Q(x)) = f_x(P(x)) + f_x(Q(x)) \quad \text{y} \quad f_x(P(x)Q(x)) = f_x(P(x))f_x(Q(x)),$$

como queríamos comprobar. ■

Observación II.6.22 Si $f_{x,n} : \mathbb{Z}[x] \to (\mathbb{Z}/n\mathbb{Z})[x]$ es el homomorfismo de anillos dado por el Corolario II.6.21, abusando de la notación, habitualmente denotaremos a $f_{x,n}(P(x))$, es decir, al polinomio resultante al considerar los coeficientes módulo n, también por $P(x)$ y diremos que consideramos $P(x)$ en $(\mathbb{Z}/n\mathbb{Z})[x]$.
Por ejemplo, si decimos que consideramos $x^3 + 6x^2 + 11x + 2$ como polinomio de $(\mathbb{Z}/3\mathbb{Z})[x]$, hay que entender que nos referimos al polinomio $x^3 + 2x + 2$ de $(\mathbb{Z}/3\mathbb{Z})[x]$.

II.6.3 El dominio $D[x]$

Queremos evitar que el grado del producto de dos polinomios sea estrictamente menor que la suma de los grados de los factores como en el Ejemplo II.6.10, para ello restringiremos nuestro estudio a anillos de polinomios con coeficientes en un dominio.

Teorema II.6.23 Sea D un dominio. Entonces se cumple que $D[x]$ es un dominio.

Demostración. Como D es un dominio, por (D.I) y (D.II), sabemos que D es un anillo conmutativo y unitario. Por las Proposiciones II.6.4 y II.6.3, sabemos que $D[x]$ es un anillo conmutativo y unitario. En otras palabras, $D[x]$ satisface (D.I) y (D.II) y sólo falta que comprobar que también verifica (D.III).

Veamos que el polinomio nulo es el único divisor del cero en $D[x]$.

Como D satisface (D.III) tenemos que 0_D es divisor de cero. Luego existe $a \in D$ con $a \neq 0$ tal que $a \cdot 0_D = 0$. Considerando el polinomio $P(x) = a \neq 0$ vemos que el polinomio nulo $N(x) = 0$ es divisor de cero en $D[x]$ porque $P(x)N(x) = 0$.
Veamos que no hay más divisores de cero a parte del polinomio nulo. Dados dos polinomios $P(x), Q(x) \in D[x]\backslash\{0\}$, podemos escribir $P(x) = \sum_{j=0}^{n} a_j x^j$ y $Q(x) = \sum_{j=0}^{m} b_j x^j$ con $a_n \neq 0$ y con $b_m \neq 0$. Por la definición del producto de polinomios:

$$P(x)Q(x) = \sum_{j=0}^{n+m} (\sum_{k=0}^{j} a_k b_{j-k}) x^j = \sum_{j=0}^{n+m-1} (\sum_{k=0}^{j} a_k b_{j-k}) x^j + a_n b_m x^{n+m}.$$

Como D verifica (D.III) y $a_n \neq 0$ y con $b_m \neq 0$, vemos que $a_n b_m \neq 0$. Por consiguiente, $P(x)Q(x) \neq 0$ y concluimos que $D[x]$ es un dominio. ■

Ejemplos II.6.24 Los anillos de polinomios $(\mathbb{Z}[x], +, \cdot)$, $(\mathbb{Z}/p\mathbb{Z}[x], +, \cdot)$ con $p \in \mathbb{N}_{\geq 1}$ primo, $(\mathbb{Q}[x], +, \cdot)$ $(\mathbb{R}[x], +, \cdot)$, $(\mathbb{C}[x], +, \cdot)$ son dominios.

Proposición II.6.25 Sea D un dominio. Entonces para todos $P(x), Q(x) \in D[x]\backslash\{0\}$, se tiene que

$$\mathrm{gr}(P(x)Q(x)) = \mathrm{gr}(P(x)) + \mathrm{gr}(Q(x)). \qquad (\textit{Comparar con la Proposición II.6.9})$$

Demostración. Dados dos polinomios $P(x), Q(x) \in D[x]\backslash\{0\}$, podemos escribir $P(x) = \sum_{j=0}^{n} a_j x^j$ y $Q(x) = \sum_{j=0}^{m} b_j x^j$ con $a_n \neq 0$ y con $b_m \neq 0$, es decir, con $\mathrm{gr}(P(x)) = n$ y con $\mathrm{gr}(Q(x)) = m$. Por la definición del producto de polinomios:

$$P(x)Q(x) = \sum_{j=0}^{n+m} (\sum_{k=0}^{j} a_k b_{j-k}) x^j = \sum_{j=0}^{n+m-1} (\sum_{k=0}^{j} a_k b_{j-k}) x^j + a_n b_m x^{n+m}.$$

Como D verifica (D.III) y $a_n \neq 0$ y con $b_m \neq 0$, vemos que $a_n b_m \neq 0$ y, por tanto, $\mathrm{gr}(P(x)Q(x)) = n + m$. ■

El siguiente resultado muestra que para conocer las unidades de $D[x]$ basta conocer las unidades de D.

Teorema II.6.26 Sea D un dominio. Entonces $U(D[x]) = U(D)$.

Nota: por la Proposición II.6.11, podemos ver D como subanillo de $D[x]$ y, rigurosamente, este ejercicio nos pide probar que $U(D[x]) = \{P(x) \in D[x] : a_0 \in U(D)$ y $a_j = 0$ si $j \in \mathbb{N}_{\geq 1}\}$.

Demostración. Dado $P(x) \in D[x]$ con $a_0 \in U(D)$ y $a_j = 0$ si $j \in \mathbb{N}_{\geq 1}$, consideramos el polinomio $Q(x)$ con $b_0 = a_0^{-1}$ y $b_j = 0$ si $j \in \mathbb{N}_{\geq 1}$. Por la definición del producto de polinomios, $P(x)Q(x)$ es el polinomio con $c_0 = 1_D$ y $c_j = 0$ si $j \in \mathbb{N}_{\geq 1}$ y por la Proposición II.6.3, sabemos que este polinomio es el neutro para el producto en $D[x]$, luego $P(x) \in U(D[x])$. En consecuencia, $\{P(x) \in D[x] : a_0 \in U(D) \text{ y } a_j = 0 \text{ si } j \in \mathbb{N}_{\geq 1}\} \subseteq U(D[x])$.

Veamos que se cumple el otro contenido, dado $P(x) = \sum_{j=0}^{n} a_j x^j \in U(D[x])$, existe otro polinomio $Q(x) = \sum_{j=0}^{m} b_j x^j \in D[x]$ tal que $P(x)Q(x) = 1$. Por la Proposición II.6.25, vemos que $\text{gr}(P(x)) + \text{gr}(Q(x)) = \text{gr}(P(x)Q(x)) = \text{gr}(1) = 0$. Por este motivo, $\text{gr}(P(x)) = \text{gr}(Q(x)) = 0$, luego $a_j = b_j = 0$ si $j \in \mathbb{N}_{\geq 1}$ y, como $P(x)Q(x) = 1$, se tiene que $a_0 b_0 = 1_D$, concluimos que $a_0 \in U(D)$. Por lo tanto, $U(D[x]) \subseteq \{P(x) \in D[x] : a_0 \in U(D) \text{ y } a_j = 0 \text{ si } j \in \mathbb{N}_{\geq 1}\}$. ■

Ejemplos II.6.27 De acuerdo con este teorema y con los resultados anteriores tenemos que $U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{\pm 1\}$ y para todo cuerpo $\mathbb{K}$ se tiene que $U(\mathbb{K}[x]) = U(\mathbb{K}) = \mathbb{K}\backslash\{0\}$.
Por otra parte, también se tiene que $U(\mathbb{R}[x,y]) = U(\mathbb{R}[x][y]) = U(\mathbb{R}[x]) = U(\mathbb{R}) = \mathbb{R}\backslash\{0\}$.

Corolario II.6.28 Sea D un dominio y $p \in D$ irreducible. Entonces el polinomio $P(x) = p$ ($a_0 = p$ y $a_j = 0$ si $j \in \mathbb{N}_{\geq 1}$) es irreducible en $D[x]$.

Demostración. Como p es irreducible $p \neq 0$ y $p \notin U(D)$, luego $P(x) \neq 0$ y, por el Teorema II.6.26, $P(x) \notin U(D[x])$.
Supongamos que existen $A(x), B(x) \in D[x]$ tales que $P(x) = A(x)B(x)$ veamos que o $A(x) \in U(D[x])$ o $B(x) \in U(D[x])$. Como $P(x) \neq 0$, $A(x) \neq 0$ y $B(x) \neq 0$ y, por la Proposición II.6.25, se tiene que

$$0 = \text{gr}(P(x)) = \text{gr}(A(x)) + \text{gr}(B(x)).$$

Por tanto, $\text{gr}(A(x)) = \text{gr}(B(x)) = 0$, es decir, existen $a, b \in D$ tales que $A(x) = a$ y $B(x) = b$. Como $P(x) = A(x)B(x)$, $p = ab$ y como p es irreducible o $a \in U(D)$ o $b \in U(D)$. De nuevo, por el Teorema II.6.26, concluimos que o $A(x) \in U(D[x])$ o $B(x) \in U(D[x])$, es decir, $P(x) = p$ es irreducible en $D[x]$. ■

Ejemplos II.6.29 Los polinomios constantes 2, 7 y 13 son irreducibles en $\mathbb{Z}[x]$ porque son irreducibles en $\mathbb{Z}$. Los polinomios $x^2 - 2$ y $x + 1$ son irreducibles en $\mathbb{Q}[x,y]$ porque son irreducibles en $\mathbb{Q}[x]$.

Finalmente, concluimos la sección probando que podemos realizar la división de polinomios en $D[x]$ siempre que el coeficiente del término de mayor grado del divisor sea una unidad en el dominio. En particular, esto nos permite realizar siempre la división por polinomios mónicos.

Teorema II.6.30 Sean D un dominio $A(x), B(x) \in D[x]$ con $\text{gr}(B(x)) = m$ y $b_m \in U(D)$. Entonces existen únicos $Q(x), R(x) \in D[x]$ tales que $A(x) = B(x)Q(x) + R(x)$ o con $R(x) = 0$ o con $\text{gr}(R(x)) < \text{gr}(B(x))$.

Demostración. EXISTENCIA. En primer lugar, observamos que si $A(x) = 0$ o si $\text{gr}(A(x)) < \text{gr}(B(x))$, tomando $Q(x) = 0$ y $R(x) = A(x)$ se cumple la igualdad.

Por consiguiente, podemos suponer que $\text{gr}(A(x)) = n \geq m = \text{gr}(B(x))$. Vamos a realizar la demostración por inducción $k = n - m = \text{gr}(A(x)) - \text{gr}(B(x))$. Escribimos:

$$A(x) = a_0 + a_1 x + \cdots + a_n x^n \quad \text{y} \quad B(x) = b_0 + b_1 x + \cdots + b_m x^m$$

Si $k = 0$, es decir, si $n = \text{gr}(A(x)) = \text{gr}(B(x)) = m$, como $b_n \in U(D)$, podemos considerar b_n^{-1}. Definimos $Q(x) := a_n b_n^{-1}$ y observamos que al considerar $R(x) := A(x) - Q(x)B(x)$ eliminamos el término de mayor grado, luego o bien se satisface que $R(x) = 0$ o bien $\text{gr}(R(x)) < \text{gr}(B(x)) = n$.

Supongamos que la propiedad se cumple para todo polinomio $\widetilde{A}(x)$ con $\ell = \mathrm{gr}(\widetilde{A}(x)) - \mathrm{gr}(B(x))$ menor que un cierto $k \in \mathbb{N}_{\geq 1}$ y veamos que se cumple para k.
Si $k = \mathrm{gr}(A(x)) - \mathrm{gr}(B(x))$, definimos $\widetilde{A}(x) := A(x) - a_n b_m^{-1} x^k B(x)$.
Si $\widetilde{A}(x) = 0$, basta tomar $Q(x) = a_n b_m^{-1} x^k$ y $R(x) = 0$.
Si $\widetilde{A}(x) \neq 0$, tenemos que $\mathrm{gr}(\widetilde{A}(x)) - \mathrm{gr}(B(x)) = \ell < k$, luego por hipótesis de inducción existen $\widetilde{Q}(x), \widetilde{R}(x) \in D[x]$ tales que

$$\widetilde{A}(x) = \widetilde{Q}(x)B(x) + \widetilde{R}(x),$$

de modo que $\widetilde{R}(x) = 0$ o $\mathrm{gr}(\widetilde{R}(x)) < \mathrm{gr}(B(x))$. Por la definición de $\widetilde{A}(x)$, los polinomios $Q(x) = a_n b_m^{-1} x^k + \widetilde{Q}(x)$ y $R(x) = \widetilde{R}(x)$ cumplen las condiciones requeridas.
En consecuencia, por el Principio de Inducción Completa podemos garantizar la existencia de cociente y resto.
UNICIDAD. Supongamos que existen polinomios $Q_1(x)$, $Q_2(x)$, $R_1(x)$ y $R_2(x)$ en $D[x]$ tales que

$$\begin{aligned} A(x) &= B(x)Q_1(x) + R_1(x) \quad \text{con} \quad R_1(x) = 0 \quad \text{o con} \quad \mathrm{gr}(R_1(x)) < \mathrm{gr}(B(x)), \\ A(x) &= B(x)Q_2(x) + R_2(x) \quad \text{con} \quad R_2(x) = 0 \quad \text{o con} \quad \mathrm{gr}(R_2(x)) < \mathrm{gr}(B(x)). \end{aligned}$$

Restando ambas ecuaciones, vemos que $(Q_1(x) - Q_2(x))B(x) + (R_1(x) - R_2(x)) = 0$. En otras palabras, se tiene que $R_2(x) - R_1(x) = (Q_1(x) - Q_2(x))B(x)$.

Si suponemos que $R_2(x) \neq R_1(x)$ y que $Q_1(x) \neq Q_2(x)$, por la Proposición II.6.8 sabemos que: $\mathrm{gr}(R_1(x) - R_2(x)) < \mathrm{gr}(B(x))$. Por otro lado, por la Proposición II.6.25, tendríamos que $\mathrm{gr}((Q_1(x) - Q_2(x))B(x)) \geq \mathrm{gr}(B(x))$. Por consiguiente, la igualdad $R_2(x) - R_1(x) = (Q_1(x) - Q_2(x))B(x)$ sería imposible.

Por tanto, $R_2(x) = R_1(x)$ o $Q_1(x) = Q_2(x)$. En el primer caso, tendríamos que se cumple la igualdad $0 = (Q_1(x) - Q_2(x))B(x)$ como $B(x)$ es no nulo por la Ley de Cancelación concluimos que $Q_1(x) = Q_2(x)$. En el segundo caso, si $Q_1(x) = Q_2(x)$ tendríamos que $R_2(x) - R_2(x) = 0$, luego $R_2(x) = R_1(x)$. Consecuentemente, el cociente y el resto son únicos. ■

Vamos ahora como las raíces de un polinomio de $D[x]$ están relacionadas con su descomposición en factores.

Teorema II.6.31 (Teorema del Resto). Sean D un dominio, $a \in D$ y $P(x) \in D[x]$. Entonces se cumple que:

(I) $P(a)$ es el resto de dividir $P(x)$ entre $x - a$.

(II) a es una raíz de P si y solamente si existe $Q(x) \in D[x]$ tal que $P(x) = (x-a)Q(x)$.

Demostración. (I) Como $x - a$ es un polinomio mónico podemos dividir $P(x)$ entre $x - a$ aplicando (DE.II) sabemos que existen $Q(x), R(x) \in D[x]$ tales que $P(x) = (x-a)Q(x) + R(x)$ o con $R(x) = 0$ o con $\mathrm{gr}(R(x)) < 1 = \mathrm{gr}(x-a)$. En otras palabras, $P(x) = (x-a)Q(x) + r$ con $r \in D$. Por el Corolario II.6.16, sabemos que la aplicación de evaluación en a es un homomorfismo de anillos luego

$$P(a) = e_a(P(x)) = e_a\Big((x-a)Q(x) + R(x)\Big) = e_a((x-a))e_a(Q(x)) + e_a(R(x)) = 0 \cdot Q(a) + r = r.$$

(II) Por (I), tenemos que a es una raíz de P si y solamente si $P(a) = 0$ si y solamente si $R(x) = 0$ si y solamente si existe $Q(x) \in D[x]$ tal que $P(x) = (x-a)Q(x)$. ■

Definición II.6.32 Sean D y D' dominios, con D subanillo de D', $1_{D'} \in D$, $a \in D'$ y $P(x) \in D[x]$, no nulo, tal que $P(a) = 0$. Por el Teorema II.6.31, sabemos que $(x-a) \mid P(x)$ en $D'[x]$. Se llama **multiplicidad de a como raíz de $P(x)$** al

$$\text{máx}\{k \in \mathbb{N}_{\geq 1} : (x-a)^k \mid P(x) \text{ en } D'[x]\}.$$

Proposición II.6.33 Sean D un dominio y $P(x) \in D[x]$ no nulo. Entonces $P(x)$ tiene a lo sumo $n = \text{gr}(P(x))$ raíces en D contadas con su multiplicidad.

Además, si D' es un dominio que contiene a D como subanillo y que $1_{D'} \in D$ entonces $P(x)$ tiene a lo sumo $n = \text{gr}(P(x))$ raíces en D' contadas con su multiplicidad.

Demostración. En primer lugar, probaremos por inducción sobre $n = \text{gr}(P(x))$ que $P(x)$ tiene a lo sumo $n = \text{gr}(P(x))$ contadas con su multiplicidad raíces en D.
Si $n = 0$, entonces $P(x) = c$ con $c \in D\backslash\{0\}$ luego $P(x)$ no tiene raíces en D.
Supongamos que la propiedad se cumple para todo polinomio de $A(x) \in D[x]$ no nulo con $\text{gr}(A(x)) = \ell < n$. Sea $P(x) \in D[x]$ un polinomio de grado $n = \text{gr}(P(x))$.
Si $P(x)$ no tiene raíces en D, entonces hemos terminado.
Si $P(x)$ tiene una raíz $a \in D$, entonces tenemos que el conjunto $\{k \in \mathbb{N}_{\geq 1} : (x-a)^k \mid P(x) \text{ en } D[x]\}$ es no vacío y, como $P(x)$ es no nulo, está acotado superiormente por la Proposición II.6.25.
Sea $m = \text{máx}\{k \in \mathbb{N}_{\geq 1} : (x-a)^k \mid P(x) \text{ en } D[x]\}$. Entonces existe $H(x) \in D[x]$ tal que $P(x) = (x-a)^m H(x)$ y con $H(a) \neq 0$, por el Teorema II.6.31. Por la Proposición II.6.25, tenemos que $n = \text{gr}(P(x)) = m + \text{gr}(H(x))$. Por **hipótesis de inducción**, como $\text{gr}(H(x)) = n - m < n$ tenemos que $H(x)$ tiene a lo sumo $n-m$ raíces contadas con su multiplicidad en D.
Toda raíz $b \neq a$ de $P(x)$ tiene que ser raíz de $H(x)$ porque $0 = P(b) = (b-a)^m H(b)$. Comprobamos que la multiplicidad de b como raíz de H es la misma que como raíz de $P(x)$ y concluimos que $P(x)$ tiene lo sumo $(n-m)+m = n$ raíces en D contadas con su multiplicidad. Por tanto, por el Principio de Inducción queda demostrado que $P(x)$ tiene a lo sumo $n = \text{gr}(P(x))$ raíces en D contadas con su multiplicidad.

Finalmente, como $D[x] \subseteq D'[x]$, podemos considerar $P(x)$ como polinomio de $D'[x]$ para deducir que $P(x)$ tiene a lo sumo $n = \text{gr}(P(x))$ raíces en D' contadas con su multiplicidad. ■

En concreto estos resultados se aplican en $\mathbb{Z}[x]$ o en $F[x][y]$ con F un cuerpo. Sin embargo, no son ciertos en $R[x]$ si R no es un dominio. Por ejemplo, x^2+3x+2 tiene cuatro raíces $(1,2,4,5)$ en $\mathbb{Z}/6\mathbb{Z}$.

II.6.4 El dominio euclídeo $F[x]$

Dado un cuerpo F sabemos que F es un dominio, ver Teorema II.4.4, y, por el Teorema II.6.23, sabemos que $F[x]$ es un dominio, en particular las propiedades de la sección anterior son ciertas aquí.

Teorema II.6.34 Sea F un cuerpo. Entonces $F[x]$ es un **dominio euclídeo** respecto a la función $\delta(P(x)) = \text{gr}(P(x))$.

Demostración. **Veamos que se cumple (DE.I)**

Dados dos polinomios en $A(x), B(x) \in F[x]\backslash\{0\}$, por la definición de grado, tenemos que si $\text{gr}(A(x)) = n$ y $\text{gr}(B(x)) = m$ podemos escribir

$$A(x) = a_0 + a_1 x + \cdots + a_n x^n \quad \text{y} \quad B(x) = b_0 + b_1 x + \cdots + b_m x^m$$

con $a_i, b_j \in F$ y $a_n \neq 0$, $b_m \neq 0$. Por la definición de del producto de polinomios:

$$A(x)B(x) = \sum_{j=0}^{n+m} (\sum_{k=0}^{j} a_k b_{j-k}) x^j = \sum_{j=0}^{n+m-1} (\sum_{k=0}^{j} a_k b_{j-k}) x^j + a_n b_m x^{n+m}.$$

Como F es un cuerpo, por el Teorema II.4.4, sabemos que F es un dominio de integridad y, por ello, que el coeficiente del término de mayor grado $a_n b_m \neq 0$, es decir, $\mathrm{gr}(A(x)B(x)) = n+m$. En resumen, se tiene que

$$\delta(A(x)) = \mathrm{gr}(A(x)) = n \leq n+m = \mathrm{gr}(A(x)B(x)) = \delta(A(x)B(x)).$$

Veamos que se cumple (DE.II)

Como F es un cuerpo, es dominio, y como $B(x) \neq 0$ vemos que $\mathrm{gr}(B(x)) = m \in \mathbb{N}$ y $b_m \neq 0$, por (F.III), se tiene que $b_m \in U(F)$, luego por el Teorema II.6.30 podemos garantizar la existencia de cociente y resto. ■

Los ejemplos clásicos de este tipo de dominios euclídeos son $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ o $(\mathbb{Z}/p\mathbb{Z})[x]$ con $p \in \mathbb{N}_{\geq 1}$ primo.

Como $F[x]$ es un dominio euclídeo sabemos por el Teorema II.5.26 y por el Teorema II.5.33, que $F[x]$ es un **dominio de ideales principales** y un **dominio de factorización única**. En particular, todas las propiedades de estos dominios se cumplen en $F[x]$. El siguiente resultado muestra la unicidad del cociente y el resto en el caso del dominio euclídeo $(F[x], \mathrm{gr})$.

Corolario II.6.35 Sea F un cuerpo y $A(x), B(x) \in F[x]$ con $B(x)$ no nulo. Entonces los polinomios existen $Q(x), R(x) \in F[x]$ tales que $A(x) = B(x)Q(x) + R(x)$ o con $R(x) = 0$ o con $\mathrm{gr}(R(x)) < \mathrm{gr}(B(x))$ son únicos.

Demostración. Como F es un cuerpo, es dominio, y como $B(x) \neq 0$ vemos que $\mathrm{gr}(B(x)) = m \in \mathbb{N}$ y $b_m \neq 0$, por (F.III), se tiene que $b_m \in U(F)$, luego por el Teorema II.6.30 podemos garantizar la existencia de cociente y resto. ■

Gracias a la conexión entre factorización y raíces dada por el Teorema II.6.31 podemos estudiar cuáles son los *irreducibles de* $F[x]$ en términos del grado. *(Nota: Como* $F[x]$ *es un D.F.U. irreducibles y primos son conceptos equivalentes).*

Corolario II.6.36 Sea F un cuerpo y $P(x) \in F[x] \backslash \{0\}$. Entonces
$P(x) \in U(F[x])$ si y solo si $\mathrm{gr}(P(x)) = 0$.

Demostración. Por el Teorema II.4.4, como F es un cuerpo, F es un dominio y por el Teorema II.6.26, sabemos que $P(x) = \sum_{j=0}^{n} a_j x^j \in U(F[x])$ si y solo si $a_0 \in U(F)$ y $a_j = 0$ para todo $j \in \mathbb{N}_{\geq 1}$. Por (F.III), sabemos que $U(F) = F \backslash \{0\}$, luego $P(x) \in U(F[x])$ si y solo si $a_0 \neq 0$ y $a_j = 0$ para todo $j \in \mathbb{N}_{\geq 1}$, es decir, si y solo si $\mathrm{gr}(P(x)) = 0$. ■

Corolario II.6.37 Sea F un cuerpo y $P(x) \in F[x] \backslash \{0\}$ con $n = \mathrm{gr}(P(x)) \in \mathbb{N}_{\geq 1}$. Entonces $P(x)$ es irreducible en $F[x]$ si y sólo si $P(x)$ no se puede expresar como el producto de dos polinomios de grado menor que n.

Demostración. Supongamos que $P(x)$ es irreducible. Si $P(x) = A(x)B(x)$, entonces o $A(x) \in U(F[x])$ o $B(x) \in U(F[x])$. Por el Corolario II.6.36, o $\mathrm{gr}(A(x)) = 0$ o $\mathrm{gr}(B(x)) = 0$. Por la Proposición II.6.25, tenemos que $n = \mathrm{gr}(A(x)) + \mathrm{gr}(B(x))$, entonces $P(x)$ no se puede expresar como producto de polinomios de grado menor que n.

Recíprocamente, supongamos que $P(x)$ no se puede expresar como el producto de dos polinomios de grado menor que n. Si $P(x) = A(x)B(x)$, entonces o $\text{gr}(A(x)) = n$ o $\text{gr}(B(x)) = n$ y, como $n = \text{gr}(A(x)) + \text{gr}(B(x))$, o $\text{gr}(B(x)) = 0$ o $\text{gr}(A(x)) = 0$. Por el Corolario II.6.36, o $A(x) \in U(F[x])$ o $B(x) \in U(F[x])$, es decir, $P(x)$ es irreducible. ■

Corolario II.6.38 Sea F un cuerpo y $P(x) \in F[x]$ con $\text{gr}(P(x)) = 1$. Entonces $P(x)$ es irreducible en $F[x]$.

Demostración. Si $P(x) = A(x)B(x)$, por la Proposición II.6.25, $1 = \text{gr}(A(x)) + \text{gr}(B(x))$, luego o o $\text{gr}(A(x)) = 0$ y $\text{gr}(B(x)) = 1$ o $\text{gr}(A(x)) = 1$ y $\text{gr}(B(x)) = 0$. En cualquier caso, $P(x)$ no se puede expresar como el producto de dos polinomios de grado menor que 1 y, por el Corolario II.6.37, concluimos que $P(x)$ es irreducible. ■

Ejemplos II.6.39 Por el Corolario II.6.38: El polinomio $x-2$ es irreducible en $\mathbb{Q}[x]$, $x+\pi$ es irreducible en $\mathbb{R}[x]$, $ix+2+3i$ es irreducible en $\mathbb{C}[x]$ y $3x+6$ es irreducible en $\mathbb{Z}/7\mathbb{Z}[x]$.

Corolario II.6.40 Sean F un cuerpo y $P(x) \in F[x]$ con grado 2 o 3. Entonces $P(x)$ es irreducible en $F[x]$ si y solo si $P(x)$ no tiene raíces en F.

Demostración. Por el Corolario II.6.37, $P(x)$ es irreducible en $F[x]$ si y sólo si $P(x)$ no se puede expresar como el producto de dos polinomios de grado menor que $\text{gr}(P(x))$. Si $\text{gr}(P(x)) = 2$, esta condición se traduce en que no puede descomponer como producto de polinomios de grado 1 y si $\text{gr}(P(x)) = 3$, esta condición se traduce en que no puede descomponer como producto de un polinomio de grado 1 y un polinomio de grado 2. En resumen, podemos decir que $P(x)$ es irreducible si y sólo si no se puede expresar como el producto de dos polinomios uno de los cuales tiene grado 1. En otras palabras, $P(x)$ es irreducible si y sólo si para todos $a, b \in F$ con $a \neq 0$ tenemos que $(ax+b) \nmid P(x)$. Equivalentemente, como F es cuerpo y todo elemento no nulo es invertible y multiplicando por a^{-1}, $P(x)$ es irreducible si y sólo si para todo $c \in F$ tenemos que $(x-c) \nmid P(x)$. Por el Teorema II.6.31, concluimos que $P(x)$ es irreducible si y sólo si $P(x)$ no tiene raíces en F. ■

Ejemplos II.6.41 Por el Corolario II.6.40: El polinomio x^2-2 es irreducible en $\mathbb{Q}[x]$, x^2+1 es irreducible en $\mathbb{R}[x]$, x^2+3 es irreducible en $\mathbb{Z}/7\mathbb{Z}[x]$.

Ejemplo II.6.42 Queremos dar la lista completa de los polinomios irreducibles de $(\mathbb{Z}/2\mathbb{Z})[x]$ de grado menor que 5.

Los polinomios irreducibles son por definición no nulos y no invertibles, por el Corolario II.6.36, hay que considerar polinomios de grado mayor o igual a 1. Los dos polinomios de grado 1, x y $x+1$ son irreducibles por el Corolario II.6.38.

Observamos que debido a que los posibles coeficientes son $0, 1$ hay 2^n polinomios de grado n en $(\mathbb{Z}/2\mathbb{Z})[x]$.

Por el Corolario II.6.40, un polinomio $P(x)$ de grado 2 o 3 es irreducible si y solo si no tiene raíces en $(\mathbb{Z}/2\mathbb{Z})$, es decir, si y solo si, $P(0) = P(1) = 1$. Por tanto, el único polinomio irreducible de grado 2 es x^2+x+1 y de grado 3 los únicos son x^3+x^2+1 y x^3+x+1.

Por el Corolario II.6.37, $P(x)$ es irreducible si y solo si $P(x)$ no se puede expresar como el producto de dos polinomios de grado menor que n. En el caso de grado 4 o 5, podemos decir, equivalentemente, que $P(x)$ es irreducible si y solo si no es divisible por un polinomio de grado 1 o de grado 2. En concreto, $P(x)$ es irreducible con $\text{gr}(P(x)) = 4$ o $\text{gr}(P(x)) = 5$ si y solo si $P(0) = P(1) = 1$ y $(x^2+x+1) \nmid P(x)$. Como $P(0) = 0$ podemos descartar los polinomios con término independiente nulo y como $P(1) = 1$ podemos descartar los polinomios con un número par de términos. De los 4 polinomios de grado 4 y de los 8 de grado 5 nos quedamos con

aquellos que no son divisibles por x^2+x+1, único polinomio de grado 2 sin factores de grado 1, para completar la lista:

$$\begin{array}{lllll} x, & x^3+x+1, & x^4+x^3+x^2+x+1, & x^5+x^4+x^3+x^2+1, & x^5+x^4+x^2+x+1, \\ x+1 & x^3+x^2+1, & x^4+x+1, & x^5+x^2+1 & x^5+x^4+x^3+x+1, \\ x^2+x+1, & x^4+x^3+1, & x^5+x^3+1, & x^5+x^3+x^2+x+1, & \end{array}$$

Ejemplo II.6.43 En $R=(\mathbb{Z}/2\mathbb{Z})[x]$ se considera $I=(x^2+x+1)$. Queremos probar que R/I es un cuerpo. Por el Ejemplo II.6.42, sabemos que x^2+x+1 es irreducible en $(\mathbb{Z}/2\mathbb{Z})[x]$. Como R es un D.E. es también un D.I.P. y, por la Proposición II.5.25, el ideal I es maximal. Por el Teorema II.4.15, R/I es un cuerpo.

El ejemplo anterior es un caso particular del siguiente resultado general que nos muestra la importancia de los polinomios irreducibles debido a su conexión con los ideales maximales y los cuerpos.

Teorema II.6.44 Sea F un cuerpo y $P(x)\in F[x]$. Entonces:

$$F[x]/\big(P(x)\big) \text{ es un cuerpo} \quad \text{si y solo si} \quad P(x) \text{ es irreducible en } F[x].$$

Demostración. Como $F[x]$ es un D.E., por el Teorema II.5.33, sabemos que es un D.I.P.. Por la Proposición II.5.25, sabemos que $P(x)$ es irreducible en $F[x]$ si y solo si el ideal $\big(P(x)\big)$ es maximal. Por el Teorema II.4.15, el ideal $\big(P(x)\big)$ es maximal si y solo si $F[x]/\big(P(x)\big)$ es un cuerpo. ■

Dados $p\in\mathbb{N}_{\geq 1}$ primo y $n\in\mathbb{N}_{\geq 1}$, empleando este teorema, podemos construir cuerpos con p^n elementos

Corolario II.6.45 Sea $p\in\mathbb{N}_{\geq 1}$ primo y $H(x)\in(\mathbb{Z}/p\mathbb{Z})[x]$ irreducible. Si $\operatorname{gr}(H(x))=n\in\mathbb{N}_{\geq 1}$, entonces $(\mathbb{Z}/p\mathbb{Z})[x]/(H(x))$ es un cuerpo con p^n elementos.

Demostración. Por el Teorema II.6.44 sabemos que $K:=(\mathbb{Z}/p\mathbb{Z})[x]/(H(x))$ es un cuerpo.
Como $(\mathbb{Z}/p\mathbb{Z})[x]$ es un D.E., la clase de todo polinomio $P(x)$ en K coincide con la clase del resto de dividir $P(x)$ entre $H(x)$ porque $P(x)-R(x)=Q(x)H(x)\in(H(x))$. En otras palabras la clase de todo polinomio $P(x)$ en K puede ponerse como la clase de un polinomio $R(x)$ con $R(x)=0$ o $\operatorname{gr}(R(x))<n$.
Si dos polinomios $A(x),B(x)$ con $\operatorname{gr}(A(x))<n$ y $\operatorname{gr}(B(x))<n$ están en la misma clase de K tenemos que $A(x)-B(x)\in(H(x))$. Como los polinomios no nulos de $(H(x))$ tiene grado mayor que n (Proposición II.6.25), la única opción es que $A(x)-B(x)=0$.
Por consiguiente, hay tantas clases en K como polinomios de grado menor que n en $(\mathbb{Z}/p\mathbb{Z})[x]$ y, como hay p posibilidades para cada coeficiente, $\#K=p^n$. ■

Ejemplo II.6.46 Queremos construir un cuerpo con 4 elementos y otro con 16. Por el Ejemplo II.6.42, sabemos que los polinomios x^2+x+1 y x^4+x^3+1 son irreducibles en $(\mathbb{Z}/2\mathbb{Z})[x]$. Por el Corolario II.6.45, sabemos que $(\mathbb{Z}/2\mathbb{Z})[x]/\big(x^2+x+1\big)$ es un cuerpo con $2^2=4$ elementos y que $(\mathbb{Z}/2\mathbb{Z})[x]/\big(x^4+x^3+1\big)$ es un cuerpo con $2^4=16$ elementos.

II.6.5 Polinomios irreducibles y primitivos en $D[x]$

De acuerdo con los resultados de las secciones anteriores, dado un dominio D y un cuerpo F estudiar la irreducibilidad de polinomios en $D[x]$ puede parecer, a priori, más complicado que que estudiar la irreducibilidad de polinomios en $F[x]$. Esta sección está encaminada a deducir propiedades de los elementos irreducibles en $D[x]$ considerándolos como elementos de $F(D)[x]$

donde D es un D.F.U. y $F(D)$ es su cuerpo de fracciones (ver Teorema II.4.17). En particular, estos resultados se aplican para $D[x]=\mathbb{Z}[x]$ y $F(D)[x]=\mathbb{Q}[x]$.

Definición II.6.47 Sean D un D.F.U. y $P(x)\in D[x]$. Decimos que es **un polinomio primitivo** si no existe un elemento irreducible de D que divida a todos los coeficientes de $P(x)$.

Ejemplos II.6.48 $3x+6x^2$ no es primitivo en $\mathbb{Z}[x]$ pero $4x^2+6x+9$ sí es primitivo en $\mathbb{Z}[x]$. $P(x,y)=x^2-5x+6+2y^2$ es primitivo en $\mathbb{Q}[x,y]=\mathbb{Q}[x,y]=(\mathbb{Q}[x])[y]$. Observamos que $P(x,y)=a_0(x)+a_1(x)y+a_2(x)y^2$ con $a_2(x)=2$, $a_1(x)=0$ y $a_0(x)=x^2-5x+6=(x-2)(x-3)$. Como 1 es un m.c.d de $a_0(x),a_1(x),a_2(x)$ en $\mathbb{Q}[x]$, $P(x,y)$ es un polinomio primitivo de $(\mathbb{Q}[x])[y]$.

Teorema II.6.49 (Lema de Gauss). El producto de dos polinomios primitivos es primitivo.

Demostración. Dados dos polinomios primitivos $P(x)=\sum_{j=0}^{n}a_jx^j$ y $Q(x)=\sum_{j=0}^{m}b_jx^j$ de $D[x]$, razonamos por reducción al absurdo y suponemos que $P(x)Q(x)=\sum_{j=0}^{n+m}c_jx^j$ no es primitivo. Por tanto, existe $p\in D$ irreducible tal que $p\mid c_j$ para todo $j\in\mathbb{N}$.

Por la Proposición II.5.12, como D es un D.F.U., p es primo. Por la Proposición II.5.9.(I), $I=(p)$ es un ideal primo. Por el Teorema II.4.15, D/I es un dominio. Por las Propiedades II.3.6, la composición del homomorfismo sobreyectivo $\pi:D\to D/I$ de paso al cociente con la inclusión canónica $\psi:D/I\to(D/I)[x]$ (Ver Proposición II.6.11) define un homomorfismo de anillos unitario, $f=(\psi\circ\pi):D\to(D/I)[x]$. Aplicando el Teorema II.6.14, para $R=D$, $S=(D/I)[x]$ y $s=x\in(D/I)[x]$ tenemos que existe un homomorfismo de anillos unitarios

$$\begin{array}{rccc} f_x: & D[x] & \longrightarrow & (D/I)[x] \\ & \displaystyle\sum_{j=0}^{n}a_jx^j & \longrightarrow & \displaystyle\sum_{j=0}^{n}f(a_j)x^j \qquad \text{con} \quad f(a_j)=a_j+I, \end{array}$$

Por consiguiente, como $c_j=pd_j$ con $d_j\in D$ tenemos que $c_j\in I$ y se cumple que

$$0=f_x(0)=f_x(P(x)Q(x))=f_x(P(x))f_x(Q(x)).$$

Por el Teorema II.6.23, $(D/I)[x]$ es dominio porque D/I es dominio. Luego o $f_x(P(x))=0$ o $f_x(Q(x))=0$. Por consiguiente, o $a_j\in(p)$ para todo $j\in\mathbb{N}$ o $b_j\in(p)$ para todo $j\in\mathbb{N}$, en otras palabras, $p\mid a_j$ para todo $j\in\mathbb{N}$ o $p\mid b_j$ para todo $j\in\mathbb{N}$, contradiciendo el hecho de que $P(x)$ y $Q(x)$ sean primitivos. ■

El estudio de la irreducibilidad de polinomio en $F[x]$ es sencillo porque se puede expresar en términos del grado como muestran los Corolarios II.6.36 y II.6.37. Si D es un D.F.U., tenemos un resultado análogo en $D[x]$ para polinomios primitivos.

Teorema II.6.50 Sea D un D.F.U. y $P(x)\in D[x]$ con $P(x)$ primitivo. Entonces

(I) Si $\mathrm{gr}(P(x))=0$, entonces $P(x)\in U(D[x])=U(D)$ (ver Teorema II.6.26).

(II) Si $n=\mathrm{gr}(P(x))\in\mathbb{N}$, tenemos que $P(x)$ es irreducible en $D[x]$ si y sólo si $P(x)$ no se puede expresar en $D[x]$ como el producto de dos polinomios de grado menor que n.

Demostración. (I) Si $\mathrm{gr}(P(x))=0$, razonamos por reducción al absurdo y suponemos que $P(x)=a\notin U(D)$. Como $P(x)\neq 0$, por (DFU.I), a descompone como producto de irreducibles. En particular, existe $p\in D$ irreducible tal que $p\mid a$, es decir, p divide a todos los coeficientes de $P(x)$, contradiciendo que $P(x)$ es primitivo.

(II) Supongamos que $P(x)$ es irreducible. Si $P(x) = A(x)B(x)$, entonces o $A(x) \in U(D[x])$ o $B(x) \in U(D[x])$. Por el Teorema II.6.26, o $A(x) = a \in U(D)$ o $B(x) = b \in U(D)$. Por tanto, o $\text{gr}(A(x)) = 0$ o $\text{gr}(B(x)) = 0$. Por la Proposición II.6.25, tenemos que $n = \text{gr}(A(x)) + \text{gr}(B(x))$, entonces o $\text{gr}(B(x)) = n$ o $\text{gr}(A(x)) = n$. En otras palabras, $P(x)$ no se puede expresar como producto de polinomios de grado menor que n.
Recíprocamente, supongamos que $P(x)$ no se puede expresar como el producto de dos polinomios de grado menor que n. Si $P(x) = A(x)B(x)$, entonces o $\text{gr}(A(x)) = n$ o $\text{gr}(B(x)) = n$ y, como $n = \text{gr}(A(x)) + \text{gr}(B(x))$, o $\text{gr}(B(x)) = 0$ o $\text{gr}(A(x)) = 0$. En cualquiera del los dos casos, $P(x) = dQ(x)$ con $d \in D$ y $\text{gr}(Q(x)) = n$.
Veamos que $d \in U(D)$. Razonamos por reducción al absurdo si $d \notin U(D)$, como $d \neq 0$, por (DFU.I) tenemos que d descompone como producto de irreducibles $d = p_1 \cdots p_k$ con $p_j \in D$ irreducible. Como $P(x) = \sum_{j=0}^{n} a_j x^j = dQ(x)$ se tiene que $d \mid a_j$ para todo $j \in \{0, \ldots, n\}$. Por tanto, tendríamos que $p_1 \mid a_j$ para todo $j \in \{0, \ldots, n\}$, contradiciendo que $P(x)$ es primitivo. En consecuencia, $d \in U(D)$ y, empleando el Teorema II.6.26, vemos que, o $A(x) \in U(D[x])$ o $B(x) \in U(D[x])$, es decir, $P(x)$ es irreducible. ■

Corolario II.6.51 Sea D un D.F.U. y $P(x) \in D[x]$ un polinomio irreducible. Entonces o bien $P(x)$ es primitivo o bien $\text{gr}(P(x)) = 0$ y $P(x) = p$ con p irreducible en D.

Demostración. Supongamos que $P(x) = \sum_{j=0}^{n} a_j x^j$ no es primitivo, entonces existe un $q \in D$ irreducible tal que $q \mid a_j$ para todo $j \in \{1, \ldots, n\}$. Escribiendo $a_j = qc_j$ vemos que $P(x) = q \cdot Q(x)$ con $Q(x) = \sum_{j=0}^{n} c_j x^j$. Recordamos que por el Teorema II.6.26 $U(D) = U(D[x])$. Como $P(x)$ es irreducible y $q \notin U(D) = U(D[x])$, tenemos que $Q(x) \in U(D[x]) = U(D)$. Por consiguiente, $Q(x) = u \in U(D)$ y $P(x) = qu$, luego $\text{gr}(P(x)) = 0$ y $P(x) = p$ con $p = qu$ irreducible en D (Observación II.5.7). ■

El siguiente teorema establece que podemos descomponer todo polinomio de $F(D)[x]$ como producto de un elemento de $F(D)$ y un polinomio primitivo de $D[x]$.

Teorema II.6.52 Sea D un D.F.U. y $F(D)$ su cuerpo de fracciones (ver Teorema II.4.17), gracias a la inclusión canónica podemos considerar todo polinomio de $D[x]$ como un polinomio de $F(D)[x]$. Entonces todo polinomio $H(x) \in F(D)[x]$ no nulo, puede expresarse como

$$H(x) = aP(x) \text{ con } a \in F(D) \text{ y } P(x) \in D[x] \text{ primitivo.}$$

Además, si $H(x) \in D[x]$ podemos tomar $a \in D$.

Demostración. Dado un polinomio $H(x) = \sum_{j=0}^{n} h_j x^j \in F(D)[x]$ sus coeficientes son de la forma $h_j = a_j/b_j$ con $a_j, b_j \in D$, $b_j \neq 0$ para todo $j \in \mathbb{N}$. Como D es un D.F.U., por la Proposición II.5.19 y la Observación II.5.20, existe $m \in D$ un m.c.m de $b_0, b_1, \ldots, b_n$. Por tanto, tenemos que $m = m_j b_j$ con $m_j \in D$ y escribimos $c_j = m_j a_j$. Multiplicando y dividiendo el coeficiente h_j por m_j y, aplicando la propiedad distributiva, se tiene que

$$H(x) = \sum_{j=0}^{n} h_j x^j = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n = \frac{c_0}{m} + \frac{c_1}{m}x + \cdots + \frac{c_n}{m}x^n = \frac{1}{m}(c_0 + c_1 x + \cdots + c_n x^n).$$

Del mismo modo, podemos garantizar que existe d un m.c.d. de $c_0, c_1, \ldots, c_n$. Por tanto, tenemos que $c_j = d_j d$ con $d_j \in D$. Escribimos $a = d/m$ y $P(x) = \sum_{j=0}^{n} d_j x^j$ y observamos que $H(x) =$

$aP(x)$.
Finalmente, comprobamos que $P(x)$ es primitivo. Si existiera $p \in D$ irreducible de modo que $p \mid d_j$ para todo $j \in \{0,1,\ldots,n\}$ tendríamos que $pd \mid c_j$ para todo $j \in \{0,1,\ldots,n\}$. Por (MCD.II), Como d es un m.c.d. de $c_0, c_1, \ldots, c_n$ se tendría que $pd \mid d$ luego $d = g(pd)$. Como d es no nulo porque $H(x)$ es no nulo, por la ley de cancelación, $1 = gp$ y tendríamos que $p \in U(D)$ contradiciendo que p es irreducible.

Finalmente, observamos que si $H(x) \in D[x]$ entonces $m = 1$ y $a \in D$. ■

Ejemplo II.6.53 Aplicando el Teorema anterior al polinomio

$$P(x) = \frac{10}{3} + \frac{15}{4}x + 5x^2 + 15x^5 \in \mathbb{Q}[x]$$

lo podemos escribir como producto de un elemento de $\mathbb{Q}$ y un polinomio primitivo de $\mathbb{Z}[x]$ como

$$P(x) = \frac{5}{12}(8 + 9x + 12x^2 + 36x^5)$$

Esta forma de escribir los polinomios de $F(D)[x]$ es única salvo producto por unidades de D.

Corolario II.6.54 Sea D un D.F.U. y $F(D)$ su cuerpo de fracciones. Entonces si un polinomio $H(x) \in F(D)[x]$ no nulo puede expresarse como $H(x) = aP_1(x)$ y como $H(x) = bP_2(x)$ con $a, b \in F(D)$ y $P_1(x), P_2(x) \in D[x]$ primitivos. Entonces:

$$\text{existe } u \in U(D) \text{ de modo que } a = ub \text{ y } P_1(x) = u^{-1}P_2(x).$$

Demostración. Suponemos que $H(x) = (d_1/m_1)P_1(x) = (d_2/m_2)P_2(x)$ con $d_1, m_1, d_2, m_2 \in D\setminus\{0\}$ y $P_1(x), P_2(x)$ en $D[x]$ primitivos. Por tanto, $Q(x) := d_1m_2P_1(x) = d_2m_1P_2(x)$ es un polinomio de $D[x]$. Como $P_1(x)$ y $P_2(x)$ son primitivos d_1m_2 y d_2m_1 son dos m.c.d. de los coeficientes de $Q(x)$. Por la Observación II.5.17, d_1m_2 está asociado a d_2m_1. Por consiguiente, existe $u \in U(D)$ de modo que $d_1m_2 = ud_2m_1$, luego $a = ub$ y, por la ley de cancelación, $P_1(x) = u^{-1}P_2(x)$. ■

El siguiente resultado nos permite estudiar la irreducibilidad de un polinomio de $D[x]$ en términos de la irreducibilidad de un polinomio de $F(D)[x]$.

Teorema II.6.55 Sea D un D.F.U., $F(D)$ su cuerpo de fracciones y $H(x) \in F(D)[x]$ con $n = \text{gr}(H(x)) \in \mathbb{N}$. Por el Teorema II.6.52, sabemos que puede expresarse como $H(x) = aP(x)$ con $a \in F(D)$ y $P(x) \in D[x]$ primitivo. Entonces se cumple que:

$$H(x) \text{ es irreducible en } F(D)[x] \text{ si y solo si } P(x) \text{ es irreducible en } D[x].$$

Demostración. Supongamos que $H(x)$ es irreducible en $F(D)[x]$. Si $P(x)$ descompone como $P(x) = A(x)B(x)$ con $A(x), B(x) \in D[x]$ tendríamos que $H(x) = aA(x)B(x)$. Por el Corolario II.6.37, como $H(x)$ es irreducible no puede descomponer como producto de polinomios de grado menor que $n = \text{gr}(H(x)) = \text{gr}(P(x))$, luego o $\text{gr}(A(x)) = n$ y $\text{gr}(B(x)) = 0$ o $\text{gr}(B(x)) = n$ y $\text{gr}(A(x)) = 0$. Por tanto, hemos probado que $P(x)$ no descompone como producto de polinomios de grado menor que $n = \text{gr}(P(x))$. Por el Teorema II.6.50, como $P(x)$ es primitivo, concluimos que $P(x)$ es irreducible en $D[x]$.
Recíprocamente, supongamos que $P(x)$ es irreducible en $D[x]$. Si $H(x) = F(x)G(x)$ con $F(x), G(x) \in F(D)[x]$. Por el Teorema II.6.52, $F(x) = fA(x)$ y $G(x) = gB(x)$ con $f, g \in F(D)$ y $A, B \in D[x]$ primitivos. Por consiguiente, tenemos que $aP(x) = H(x) = fgA(x)B(x)$. Por el Teorema II.6.49, sabemos que $A(x)B(x)$ es un polinomio primitivo y, por el Corolario II.6.54, sabemos que existe $u \in U(D)$ tal que $a = u(fg)$ y que $P(x) = u^{-1}A(x)B(x)$. Como $P(x)$ es irreducible, por

el Teorema II.6.50, o $\text{gr}(A(x)) = n$ o $\text{gr}(B(x)) = n$, por tanto, o $\text{gr}(F(x)) = n$ o $\text{gr}(G(x)) = n$. En consecuencia, $H(x)$ no descompone como producto de polinomios de grado menor y, por el Corolario II.6.37, concluimos que $H(x)$ es irreducible en $F(D)[x]$. ■

Corolario II.6.56 Sea D un D.F.U. y $F(D)$ su cuerpo de fracciones. Dado $Q(x) \in D[x]$ primitivo con $n = \text{gr}(Q(x)) \in \mathbb{N}$. Entonces $Q(x)$ es irreducible en $D[x]$ si y solamente si $Q(x)$ es irreducible en $F(D)[x]$.

Demostración. Observamos que podemos descomponer $Q(x)$ en la forma del Teorema II.6.52 como $Q(x) = 1 \cdot Q(x)$, es decir, con $H(x) = Q(x)$, $a = 1$ y $P(x) = Q(x)$. Por tanto, aplicando el Teorema II.6.55, podemos concluir que $P(x)$ es irreducible en $D[x]$ si y solamente si $P(x)$ es irreducible en $F(D)[x]$. ■

Gracias a esta relación entre polinomios primitivos de $D[x]$ e irreducibles en $F(D)[x]$, podemos que $F(D)[x]$ es un D.F.U. para probar que si D es un D.F.U., entonces $D[x]$ es un D.F.U.

Teorema II.6.57 Si D es un D.F.U., entonces $D[x]$ es un D.F.U.

Demostración. **Existencia de la descomposición (DFU.I)**

Dado $P(x) \in D[x] \backslash \{0_D\}$ y $P(x) \notin U(D[x]) = U(D)$ (ver Teorema II.6.26).

Distinguimos dos casos:

(a) Si $\text{gr}(P(x)) = 0$, tenemos que $P(x) = a$ con $a \in D$. Como D es un D.F.U., existen $p_1, \ldots, p_k$ irreducibles en D tales que $a = p_1 \cdots p_k$. Por el Corolario II.6.28, tenemos que p_j es irreducible en $D[x]$, luego $P(x) = p_1 \cdots p_k$ descompone como producto de irreducibles.

(b) Si $\text{gr}(P(x)) \in \mathbb{N}$, como $D[x] \subseteq F(D)[x]$ podemos considerar $P(x)$ como un polinomio de $F(D)[x]$. Como $F(D)$ es un cuerpo $F(D)[x]$ es un D.E. y, por tanto, un D.F.U. Como $\text{gr}(P(x)) \in \mathbb{N}$, por el Corolario II.6.36, sabemos que $P(x) \notin U(F(D)[x])$ y, por (DFU.I), existen polinomios irreducibles $H_1(x), \ldots, H_k(x)$ en $F(D)[x]$ tales que $P(x) = H_1(x) \cdots H_k(x)$. Observamos que, como $H_j(x)$ es irreducible en $F(D)[x]$, se cumple que $\text{gr}(H_j(x)) \in \mathbb{N}$ por el el Corolario II.6.36. Aplicando el Teorema II.6.52 a cada uno de estos polinomios sabemos que pueden expresarse como $H_j(x) = h_j Q_j(x)$ con $h_j \in F(D)$ y $Q_j \in D[x]$ primitivo para todo $j \in \{1, \ldots, k\}$. Por el Teorema II.6.55, como H_j es irreducible, Q_j es irreducible en $D[x]$. En resumen, podemos escribir

$$P(x) = h_1 \cdots h_k Q_1(x) \cdots Q_k(x) \text{ con } h_j \in F(D) \text{ y } Q_j(x) \in D[x] \text{ irreducible y primitivo.}$$

Como $P(x) \in D[x]$, por el Teorema II.6.52, se tiene que $P(x) = dR(x)$ con $R(x) \in D[x]$ primitivo. Por el Teorema II.6.49, sabemos que el producto de polinomios primitivos es primitivo luego $Q(x) = Q_1(x) \cdots Q_k(x)$ es primitivo. Si $h = h_1 \cdots h_k$, observamos que $dR(x) = P(x) = hQ(x)$. Por el Corolario II.6.54, existe $u \in U(D)$, tal que $h = ud$ y que $Q(x) = u^{-1}R(x)$ y deducimos que $h \in D$.

Si $h \in U(D)$, entonces $hQ_1(x)$ es irreducible (Observación II.5.7) y $P(x)$ descompone como producto de irreducibles.

Si $h \notin U(D)$, como D es un D.F.U. entonces existen $q_1, \ldots, q_\ell$ irreducibles en D tales que $h = q_1 \cdots q_\ell$. Por el Corolario II.6.28, tenemos que q_j es irreducible en $D[x]$, luego $P(x) = q_1 \cdots q_\ell Q_1(x) \cdots Q_k(x)$ descompone como producto de irreducibles.

Unicidad de la descomposición (DFU.II) Dados $A_i(x), A_j(x)$ con $i, j \in \mathbb{N}$ elementos irreducibles en $D[x]$, tales que

$$A_1(x)A_2(x) \cdots A_n(x) = B_1(x)B_2(x) \cdots B_m(x).$$

Por el Corolario II.6.51, sabemos que o bien $\mathrm{gr}(A_i(x)) = 0$ y $A_i(x) = p_i$ irreducible o bien $A_i(x) = P_i(x)$ es primitivo. Análogamente, bien $\mathrm{gr}(B_j(x)) = 0$ y $B_j(x) = b_j$ irreducible o bien $B_j(x) = Q(x)_j$ es primitivo. Reordenando los factores podemos escribir

$$p_1 p_2 \cdots p_\ell P_{\ell+1}(x) \cdots P_n(x) = q_1 q_2 \cdots q_k Q_{k+1}(x) Q_2(x) \cdots Q_m(x),$$

con $p_i, q_j \in D$ irreducibles y $P_i(x), Q_j(x)$ irreducibles y primitivos en $D[x]$.

Por el Teorema II.6.49, tenemos que $P(x) := P_{\ell+1}(x) \cdots P_n(x)$ y $Q(x) := Q_{k+1}(x) \cdots Q_m(x)$ son polinomios primitivos de $D[x]$. Denotamos por $p = p_1 \cdots p_\ell$ y por $q = q_1 \cdots q_k$ y se tiene que $pP(x) = qQ(x)$. Por el Corolario II.6.54, existe $u \in U(D)$, tal que $p = uq$ y que $P(x) = u^{-1}Q(x)$.

Como D es un D.F.U., $p_1 \cdots p_\ell = uq_1 \cdots q_k$ y con p_i, q_j irreducibles, por (DFU.II), $\ell = k$ existe $\tau \in S_\ell$ tal que $p_i \sim q_{\tau(i)}$ en D. Como $U(D) = U(D[x])$, p_i es asociado a $q_{\tau(i)}$ también en $D[x]$.

Como $P_i(x), Q_j(x)$ irreducibles y primitivos en $D[x]$, por el Teorema II.6.50, se tiene que $\mathrm{gr}(P_j(x)) \in \mathbb{N}_{\geq 1}$ y $\mathrm{gr}(Q_j(x)) \in \mathbb{N}_{\geq 1}$ y, por el Corolario II.6.56, $P_i(x), Q_j(x)$ son irreducibles en $F(D)[x]$ para todo $i \in \{\ell+1, \ldots, n\}$ y todo $j \in \{\ell+1, \ldots, m\}$.
Como $F(D)[x]$ es un D.F.U. y como $P_{\ell+1}(x) \cdots P_n(x) = u^{-1}Q_{\ell+1}(x) \cdots Q_m(x)$, por (DFU.II), $m = n$ y todo $P_i(x)$ es asociado a algún $Q_j(x)$ en $F(D)[x]$. En otras palabras, se tiene que para todo $i \in \{\ell+1, \ldots, n\}$ existe $j \in \{\ell+1, \ldots, n\}$ y $f \in U(F(D)[x]) = U(F(D))$ tal que $P_i(x) = fQ_j(x)$. Como $P_i(x)$ y $Q_j(x)$ son primitivos, por el Corolario II.6.54, concluimos que $f \in U(D) = U(D[x])$, luego $P_i(x)$ es asociado a algún $Q_j(x)$ en $D[x]$.

En resumen, $n = m$ y existe $\sigma \in S_n$ tal que $A_i(x) \sim B_{\sigma(i)}(x)$ en $D[x]$ para todo $i \in \{1, 2, \ldots n\}$, es decir, se satisface (DFU.II). ■

Ejemplos II.6.58 (1) Tenemos que $\mathbb{Z}[x]$ es un D.F.U. En el Ejemplo II.5.30 hemos probado que $\mathbb{Z}$ es un D.E. Por tanto, por el Teorema II.5.33 y por el Teorema II.5.26 tenemos que $\mathbb{Z}$ es un D.F.U. Por el Teorema II.6.57, concluimos que $\mathbb{Z}[x]$ es un D.F.U.
(2) Dado F un cuerpo $F[x]$ es un D.E., por el Teorema II.6.34, luego por el Teorema II.5.33 y por el Teorema II.5.26 tenemos que $F[x]$ es un D.F.U. Finalmente, por el Teorema II.6.57 concluimos que $F[x, y]$ es un D.F.U. (ver Observación II.6.6).

II.6.6 Criterios de irreducibilidad

En esta sección, probaremos algunos resultados que nos dan condiciones suficientes, y sencillas de comprobar, que aseguran que un polinomio es irreducible en $D[x]$. Comenzaremos por un teorema que generaliza un resultado que que aparece en la mayoría de los textos de secundaria: 'toda raíz entera de un polinomio con coeficientes enteros debe dividir al término independiente'.

Teorema II.6.59 (Teorema de la raíz racional). Sean D un D.F.U., $P(x) = \sum_{j=0}^{n} a_j x^j \in D[x]$ con $n \in \mathbb{N}_{\geq 1}$ y $a_n \neq 0$. Dado $f \in F(D)$ se puede escribir como $f = r/s$ con $r, s \in D$ de modo que 1_D es un m.c.d. de r y s (primos relativos).
Se tiene que si $P(r/s) = 0$, entonces $r \mid a_0$ y $s \mid a_n$.

Demostración. Como $P(r/s) = \sum_{j=0}^{n} a_j (r/s)^j = 0$, observamos que

$$a_n r^n + s a_{n-1} r^{n-1} + \cdots + s^{n-1} a_1 r + s^n a_0 = 0.$$

Por tanto, se tiene que $s \mid a_n r^n$ y que $r \mid s^n a_0$. Como $r, s \in D$ son primos relativos, deducimos que $s \mid a_n$ y que $r \mid a_0$ por las propiedades del máximo común divisor. ■

Ejemplo II.6.60 Queremos probar que $P(x) = 8x^3 - 6x + 1$ es irreducible en $\mathbb{Q}[x]$. Como $\mathrm{gr}(P(x)) = 3$, por el Corolario II.6.40, sabemos que $P(x)$ es irreducible si y solo si no tiene raíces en $\mathbb{Q}$. Por el Teorema de la raíz racional, las únicas raíces racionales posibles de $P(x)$ son $\pm 1, \pm 1/2, \pm 1/4, \pm 1/8$. Comprobamos que ninguno de estos 8 elementos es raíz y concluimos que $P(x)$ es irreducible en $\mathbb{Q}[x]$.

Teorema II.6.61 (Criterio de irreducibilidad módulo p). Sean D un D.F.U., y $P(x) = \sum_{j=0}^{n} c_j x^j \in D[x]$ primitivo y con $\mathrm{gr}(P(x)) = n \in \mathbb{N}_{\geq 1}$. Supongamos que existe $p \in D$ irreducible tal que $p \nmid c_n$.
Denotamos por $I = (p)$ el ideal primo generado por p, si $\overline{P(x)} = f_x(P(x)) \in (D/I)[x]$ es el polinomio al considerar los coeficientes módulo I (ver la demostración del Teorema II.6.49). Entonces se cumple que

Si $\overline{P(x)}$ es irreducible en $(D/I)[x]$, entonces $P(x)$ es irreducible en $D[x]$.

Demostración. Del mismo modo que en la prueba del Teorema II.6.49, la aplicación:

$$\begin{array}{rccc} f_x: & D[x] & \longrightarrow & (D/I)[x] \\ & P(x) = \displaystyle\sum_{j=0}^{n} c_j x^j & \longrightarrow & \overline{P(x)} = \displaystyle\sum_{j=0}^{n} \overline{c_j} x^j \qquad \text{con} \quad \overline{c_j} = c_j + I, \end{array}$$

es un homomorfismo de anillos unitarios. Si $P(x) = A(x)B(x)$ con $A(x) = \sum_{j=0}^{r} a_j x^j, B(x) = \sum_{j=0}^{s} b_j x^j \in D[x]$, tenemos que $\overline{P(x)} = \overline{A(x)B(x)}$. Como $\overline{P(x)}$ es irreducible en $(D/I)[x]$ o $\overline{A(x)} \in U((D/I)[x]) = U(D/I)$ o $\overline{B(x)} \in U(D/I)$ porque D/I es dominio (Ver Teorema II.6.26). Por consiguiente, o $\mathrm{gr}(\overline{A(x)}) = 0$ o $\mathrm{gr}(\overline{B(x)}) = 0$.
Como $p \nmid c_n$, $p \nmid a_r b_s$, luego $p \nmid a_r$ y $p \nmid b_s$. Por tanto, $r = \mathrm{gr}(A(x)) = \mathrm{gr}(\overline{A(x)})$ y $s = \mathrm{gr}(B(x)) = \mathrm{gr}(\overline{B(x)})$. Junto con la información anterior, deducimos que o $r = 0$ o $s = 0$, es decir, $P(x)$ no puede expresarse como el producto de dos polinomios de grado menor que n. Como $P(x)$ es primitivo, por el Teorema II.6.50, concluimos que $P(x)$ es irreducible en $D[x]$. ■

Ejemplo II.6.62 Queremos probar que $P(x) = 25x^5 + 9x^3 + 81x^2 + 121x + 49$ es irreducible en $\mathbb{Q}[x]$. Como $P(x)$ es primitivo (un m.c.d. de sus coeficientes es 1) basta probar que es irreducible en $\mathbb{Z}[x]$ (Corolario II.6.56). Como $2 \nmid 25$ podemos estudiar la irreducibilidad del polinomio resultante al considerar los coeficientes en $\mathbb{Z}/2\mathbb{Z}$. Tenemos que $\overline{P(x)} = x^5 + x^3 + x^2 + x + 1$ es irreducible en $\mathbb{Z}/2\mathbb{Z}$ por el Ejemplo II.6.42. Por consiguiente, aplicando el Criterio de Irreducibilidad módulo 2, deducimos que $P(x)$ es irreducible en $\mathbb{Z}[x]$.

Teorema II.6.63 (Criterio de Eisenstein). Sea D un D.F.U., y $P(x) = \sum_{j=0}^{n} c_j x^j \in D[x]$ primitivo con $\mathrm{gr}(P(x)) = n \in \mathbb{N}_{\geq 1}$. Supongamos que existe $p \in D$ irreducible tal que:

(EIS.1) $p \mid c_j$ para todo $j < n$,

(EIS.2) $p \nmid c_n$,

(EIS.3) $p^2 \nmid c_0$.

Entonces $P(x)$ es irreducible en $D[x]$.

Demostración. Supongamos que $P(x) = A(x)B(x)$ con $A(x) = \sum_{j=0}^{r} a_j x^j$ y $B(x) = \sum_{j=0}^{s} b_j x^j$ en $D[x]$ con $n = r + s$.
Por la definición del producto de polinomios $c_j = \sum_{k=0}^{j} a_k b_{j-k}$ para todo $j \in \{0, 1, \ldots, n\}$. En particular, $c_n = a_r b_s$, por (EIS.2), se tiene que $p \nmid a_r b_s$, luego $p \nmid a_r$ y $p \nmid b_s$.

Por otro lado, $c_0 = a_0 b_0$. Por (EIS.3), como $p^2 \nmid a_0 b_0$, p no divide a a_0 y a b_0 a la vez. Por (EIS.1), $p \nmid a_0 b_0$, es decir, p divide a uno y solo a uno de los factores a_0, b_0. Supongamos que $p \mid a_0$ y $p \nmid b_0$, análogo si $p \mid b_0$ y $p \nmid a_0$. Como $p \nmid a_r$ y $p \mid a_0$ existe un $m \in \{1, \ldots, r\}$ tal que $p \mid a_j$ para $j \in \{0, \ldots, m-1\}$ y que $p \nmid a_m$. Observamos que

$$c_m = a_m b_0 + b_{n-1} a_{m-1} + \cdots + a_1 b_{m-1} + a_0 b_m.$$

Si $m < n$, por (EIS.1) $p \mid c_m$ y por la hipótesis sobre a_j, $p \mid (b_{n-1} a_{m-1} + \cdots + a_1 b_{m-1} + a_0 b_m)$. Por consiguiente, $p \mid a_m b_0$, como p es irreducible y D es un D.F.U., p es primo y se tiene que o $p \mid a_m$ o $p \mid b_0$ pero ninguna de estas dos condiciones es posible. En consecuencia, como $m \leq r \leq n$, la única posibilidad es que $n = m = r$.

En resumen, $P(x)$ no descompone como producto de dos polinomios de grado menor que n. Como $P(x)$ es primitivo, por el Teorema II.6.50, concluimos que $P(x)$ es irreducible en $D[x]$. ■

Ejemplos II.6.64 (1) Queremos probar que el polinomio $H(x) = (9/10)x^3 + (6/5)x - (9/5)$ es irreducible en $\mathbb{Q}[x]$. Observamos que podemos escribir $H(x) = (1/10)(9x^3 + 12x - 18) = (3/10)(3x^3 + 4x - 6)$. Como $P(x) := 3x^3 + 4x - 6$ es primitivo (un m.c.d. de sus coeficientes es 1) basta probar que es irreducible en $\mathbb{Z}[x]$ (Teorema II.6.55) para deducir que $H(x)$ es irreducible en $\mathbb{Q}[x]$. Podemos aplicar el Criterio de Eisenstein para $p = 2$, como $2 \mid (-6)$ y $2 \mid 4$, pero $2 \nmid 3$ y $2^2 = 4 \nmid 6$, deducimos que $P(x)$ es irreducible en $\mathbb{Z}[x]$.

(2) Queremos probar que $P(x,y) = x^2 - 5x + 6 + 2y^2$ es irreducible en $\mathbb{Q}[x,y]$. Por definición sabemos que $\mathbb{Q}[x,y] = (\mathbb{Q}[x])[y]$, como $\mathbb{Q}$ es un cuerpo $\mathbb{Q}[x]$ es un D.E. y por los Teoremas II.5.33 y II.5.26, $\mathbb{Q}[x]$ es un D.F.U. Observamos que $P(x,y) = a_0(x) + a_1(x)y + a_2(x)y^2$ con $a_2(x) = 2$, $a_1(x) = 0$ y $a_0(x) = x^2 - 5x + 6 = (x-2)(x-3)$. Como 1 es un m.c.d de $a_0(x), a_1(x), a_2(x)$ en $\mathbb{Q}[x]$, $P(x,y)$ es un polinomio primitivo de $(\mathbb{Q}[x])[y]$. Comprobamos es posible aplicar el Criterio de Eisenstein con $p = (x-3)$, que es irreducible en $\mathbb{Q}[x]$ (ver Corolario II.6.38), y concluimos que $P(x,y)$ es irreducible en $\mathbb{Q}[x,y]$.

Teorema II.6.65 (Criterio de Traslación). Sea D un dominio, $P(x) \in D[x]$ y $a \in D$. Entonces:

$$P(x) \text{ es irreducible en } D[x] \text{ si y solo si } P(x+a) \text{ es irreducible en } D[x].$$

Demostración. Consideramos el homomorfismo de anillos identidad de $f = id : D \to D$. Para $R = D$ y $S = D[x]$, aplicamos el Teorema II.6.14 dos veces, una con $s = x + a$ y otra con $s = x - a$, y vemos que

$$\begin{array}{rccc} f_{x+a}: & D[x] & \longrightarrow & D[x] \\ & \displaystyle\sum_{j=0}^{n} a_j x^j & \longrightarrow & \displaystyle\sum_{j=0}^{n} a_j (x+a)^j \end{array} \qquad \begin{array}{rccc} f_{x-a}: & D[x] & \longrightarrow & D[x] \\ & \displaystyle\sum_{j=0}^{n} a_j x^j & \longrightarrow & \displaystyle\sum_{j=0}^{n} a_j (x-a)^j \end{array}$$

son homomorfismos de anillos.

Supongamos que $P(x)$ es irreducible en $D[x]$. Si $P(x+a) = A(x)B(x)$, aplicando el homomorfismo f_{x-a}, por (HA.II), tendríamos que $P(x) = f_{x-a}(P(x+a)) = A(x-a)B(x-a)$. Como $P(x)$ es irreducible en $D[x]$ o $A(x-a) = u \in U(D[x]) = U(D)$ o $B(x-a) = u \in U(D[x]) = U(D)$ (ver Teorema II.6.26). Como para todo $d \in D$, $f_{x+a}(d) = d$, tenemos que o $A(x) = A(x-a) = u \in U(D)$ o $B(x) = B(x-a) = u \in U(D)$. En otras palabras, $P(x+a)$ es irreducible en $D[x]$.

Análogamente, se razona si suponemos que $P(x+a)$ es irreducible en $D[x]$. ■

Ejemplo II.6.66 Queremos probar que $P(x) = 8x^3 - 6x + 1$ es irreducible en $\mathbb{Q}[x]$. Observamos que

$$P(x+1) = 8(x+1)^3 - 6(x+1) + 1 = 8(x^3 + 3x^2 + 3x + 1) - 6x - 5 = 8x^3 + 24x^2 + 18x + 3.$$

Aplicamos el Criterio de Eisenstein a $P(x+1)$ para $p = 3$, $D = \mathbb{Z}$ y $F(D) = \mathbb{Q}$ y concluimos que $P(x+1)$ es irreducible en $\mathbb{Q}[x]$. Por el Criterio de Traslación, $P(x) = 8x^3 - 6x + 1$ es irreducible en $\mathbb{Q}[x]$.

Para completar la información de estos apuntes consultar las referencias: [5], [9] [11], [12], [15].

Ejercicio II.6.67 Probar que $2x + 1$ es una unidad en $(\mathbb{Z}/4\mathbb{Z})[x]$.

Ejercicio II.6.68 Probar que $x^2 + 3x + 2$ tiene 4 raíces en $\mathbb{Z}/6\mathbb{Z}$. ¿Cuáles son las raíces de $x^4 - 5x^2 + 4$ en $\mathbb{Z}/6\mathbb{Z}$?

Ejercicio II.6.69 ¿Cuántos polinomios existen en $(\mathbb{Z}/3\mathbb{Z})[x]$ tales que $f(a) = 0$ para todo $a \in \mathbb{Z}/3\mathbb{Z}$?

Ejercicio II.6.70 Determinar un polinomio en $\mathbb{Z}[x]$ tal que $f(-1/2) = f(1/3) = 0$.

Ejercicio II.6.71 Probar que $\mathbb{Q}[x]/(x^2 - 2) \approx \mathbb{Q}[\sqrt{2}]$.

Ejercicio II.6.72 Probar que para cada p primo:

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)) \qquad \text{en} \qquad \mathbb{Z}/p\mathbb{Z}[x].$$

Deducir el **Teorema de Wilson**: p es primo si y sólo si $(p-1)! \equiv -1 (\text{mód}\, p)$. Calcular el resto de dividir 98! por 101 y probar que $(50!)^2 \equiv -1 \,(\text{mód}\, 101)$.

Ejercicio II.6.73 Construir un cuerpo con 25 elementos. ¿Existe un cuerpo con 21 elementos? ¿y un dominio con 21 elementos?

Ejercicio II.6.74 Probar que $\mathbb{F}_4 = (\mathbb{Z}/2\mathbb{Z})[x]/(x^2 + x + 1)$ es un cuerpo con cuatro elementos. Probar que $\mathbb{Z}[i]/(2)$ es un anillo con cuatro elementos ¿Es cuerpo?¿Es dominio? Construir las tablas aditivas y multiplicativas de los anillos $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +, \cdot)$ y $(\mathbb{F}_4, +, \cdot)$, $(\mathbb{Z}[i]/(2), +, \cdot)$. ¿Son anillos isomorfos?

Ejercicio II.6.75 Si D es un D.I.P. ¿es $D[x]$ un D.I.P.?

Ejercicio II.6.76 Dado un cuerpo F y S un subgrupo finito de $(F \setminus \{0\}, \cdot)$. Probar que $(S, \cdot)$ es un grupo cíclico.

Ejercicio II.6.77 Dado $p \in \mathbb{N}_{\geq 1}$ primo probar que $(U(\mathbb{Z}/p\mathbb{Z}), \cdot)$ es cíclico.
Observe que cuando p no es primo el grupo puede no ser cíclico [6, 10]

Ejercicio II.6.78 Probar que $\mathbb{R}[x]/(x^2 + 1)$ es un cuerpo.

Ejercicio II.6.79 En $(\mathbb{Z}/3\mathbb{Z})[x]$ se consideran $P(x)=x^3+x^2+x+1$, $Q(x)=x^4+x^3+2x^2+x+1$ e $I=(P(x),Q(x))$. Probar que $(\mathbb{Z}/3\mathbb{Z})[x]/I$ es un cuerpo. ¿Cuántos elementos tiene?¿Cuál es el inverso de $x+I$?

Ejercicio II.6.80 Sea F un cuerpo y $P(x)\in F[x]$ de grado $n\in\mathbb{N}_{\geq 1}$. Probar que cada clase distinta de 0 en $F[x]/(P(x))$ contiene un único mónico polinomio de grado $<n$.

Ejercicio II.6.81 En $(\mathbb{Z}/3\mathbb{Z})[x]$ consideramos el polinomio $P(x)=x^3+x^2+x+2$ y el cociente $R=(\mathbb{Z}/3\mathbb{Z})[x]/(P(x))$. ¿Cuántos elementos tiene el anillo R ?¿Es R un cuerpo?

Ejercicio II.6.82 Teniendo en cuenta el orden del grupo $U(R)$ del ejercicio anterior, probar que x^2+1 no tiene ninguna raíz en R. ¿Cuántas raíces tiene en R el polinomio $x^{13}-1$?¿y $x^{13}+1$?

Ejercicio II.6.83 Sean $P(x),Q(x)\in\mathbb{Z}[x]$ polinomios con $Q(x)$ mónico. Si $Q|P$ en $\mathbb{Q}[x]$ probar que $Q|P$ en $\mathbb{Z}[x]$.

Ejercicio II.6.84 (Polinomios irreducibles con coeficientes reales). El objetivo de este ejercicio es probar que los polinomios irreducibles en $\mathbb{R}[x]$ tienen grado 1 o 2.

(I) Probar que todo polinomio de $\mathbb{R}[x]$ grado 1 es irreducible y que algunos polinomios de grado 2 son irreducibles.

(II) Sea $P(x)\in\mathbb{R}[x]$. Definiendo un automorfismo adecuado probar que $z\in\mathbb{C}$ es una raíz de $P(x)$ si y sólo si su conjugado $\overline{z}$ es una raíz de $P(x)$.

(III) Enunciar el Teorema Fundamental del Álgebra.

(IV) Probar que todo polinomio de $\mathbb{R}[x]$ grado impar mayor o igual que 3 es reducible.

(V) Probar que todo polinomio de $\mathbb{R}[x]$ grado par mayor que 2 es reducible.

Ejercicio II.6.85 ¿Es x^5-12x^2+6 irreducible en $\mathbb{Z}[x]$? ¿y en $\mathbb{Q}[x]$?

Ejercicio II.6.86 Determinar si los siguiente polinomios son irreducibles o no en $\mathbb{Q}[x]$:

$$Q_1(x)=x^3-10 \quad Q_2(x)=x^3+3x^2-6x+3 \quad Q_3(x)=x^3+3x^2-6x+9 \quad Q_4(x)=x^3-3x+4.$$

Ejercicio II.6.87 Determinar si los siguiente polinomios de $\mathbb{Z}[x]$ son primitivos en $\mathbb{Z}[x]$, irreducibles en $\mathbb{Z}[x]$, irreducibles en $\mathbb{Q}[x]$ y/o irreducibles en $\mathbb{R}[x]$:

$$P_1(x)=2x^3+6, \quad P_2(x)=x^2-3, \quad P_3(x)=x^2+1,$$

$$P_4(x)=6x^2-x-1, \quad P_5(x)=2x^3-x^2-x-3.$$

Ejercicio II.6.88 En $\mathbb{Z}[x]$, el anillo de los polinomios con coeficientes enteros, consideramos el ideal $I=(10,x-3)$ y el anillo cociente $A=\mathbb{Z}[x]/I$.

(1) Probar que $x+I=3+I$ y deducir que para todo elemento $P(x)$ de $\mathbb{Z}[x]$ existe $k\in\mathbb{Z}$ tal que $P(x)+I=k+I$.
(2) Probar que $Q(x)=6x^3+5x^2+8x+12$ es irreducible en $\mathbb{Z}[x]$.
(3) Encuentra el inverso de $Q(x)+I$ en A.

Ejercicio II.6.89 En el anillo de los polinomios con coeficientes racionales, $\mathbb{Q}[x]$, consideramos: $P_1(x) = (3/4)x^7 + 36x - 18$ y $P_2(x) = (4/3)x^3 + 4x^2 - (40/3)x - 32$ de $\mathbb{Q}[x]$.

(1) Probar que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ y que $P_2(x)$ no es irreducible en $\mathbb{Q}[x]$.
(2) Determinar si $R_1 = \mathbb{Q}[x]/(P_1(x))$ y $R_2 = \mathbb{Q}[x]/(P_2(x))$ son o no son cuerpos.
(3) Encuentra en R_1 el inverso de $((x-2)/200) + (P_1(x))$.

Ejercicio II.6.90 En $\mathbb{Z}/3\mathbb{Z}[x]$, consideramos los polinomios

$$P_1(x) = x^4 + 2x^3 + 2x + 2, \qquad P_2(x) = x^4 + x^3 + x^2 + x + 1, \qquad P_3(x) = x^3 + x + 2.$$

(I) Determinar, razonadamente, la lista completa de polinomios irreducibles de grado menor o igual que 2 de $\mathbb{Z}/3\mathbb{Z}[x]$.

(II) ¿Es $R_1 = \mathbb{Z}/3\mathbb{Z}[x]/(P_1(x))$ un dominio? ¿Es $R_2 = \mathbb{Z}/3\mathbb{Z}[x]/(P_2(x))$ un cuerpo?

(III) Hallar, si existe, el inverso para el producto de $x^2 + 1 + (P_2(x))$ en R_2.

(IV) Consideramos el ideal $I = (P_1(x), P_3(x))$ de $\mathbb{Z}/3\mathbb{Z}[x]$. Determinar si I es principal o no y, en caso de ser principal, encontrar un polinomio $P(x) \in \mathbb{Z}/3\mathbb{Z}[x]$ tal que $I = (P(x))$.

(V) Probar que $I/(P_1(x)) \approx (P_3(x))/(x^5 + 2x^3 + 2x^2 + x + 2)$.

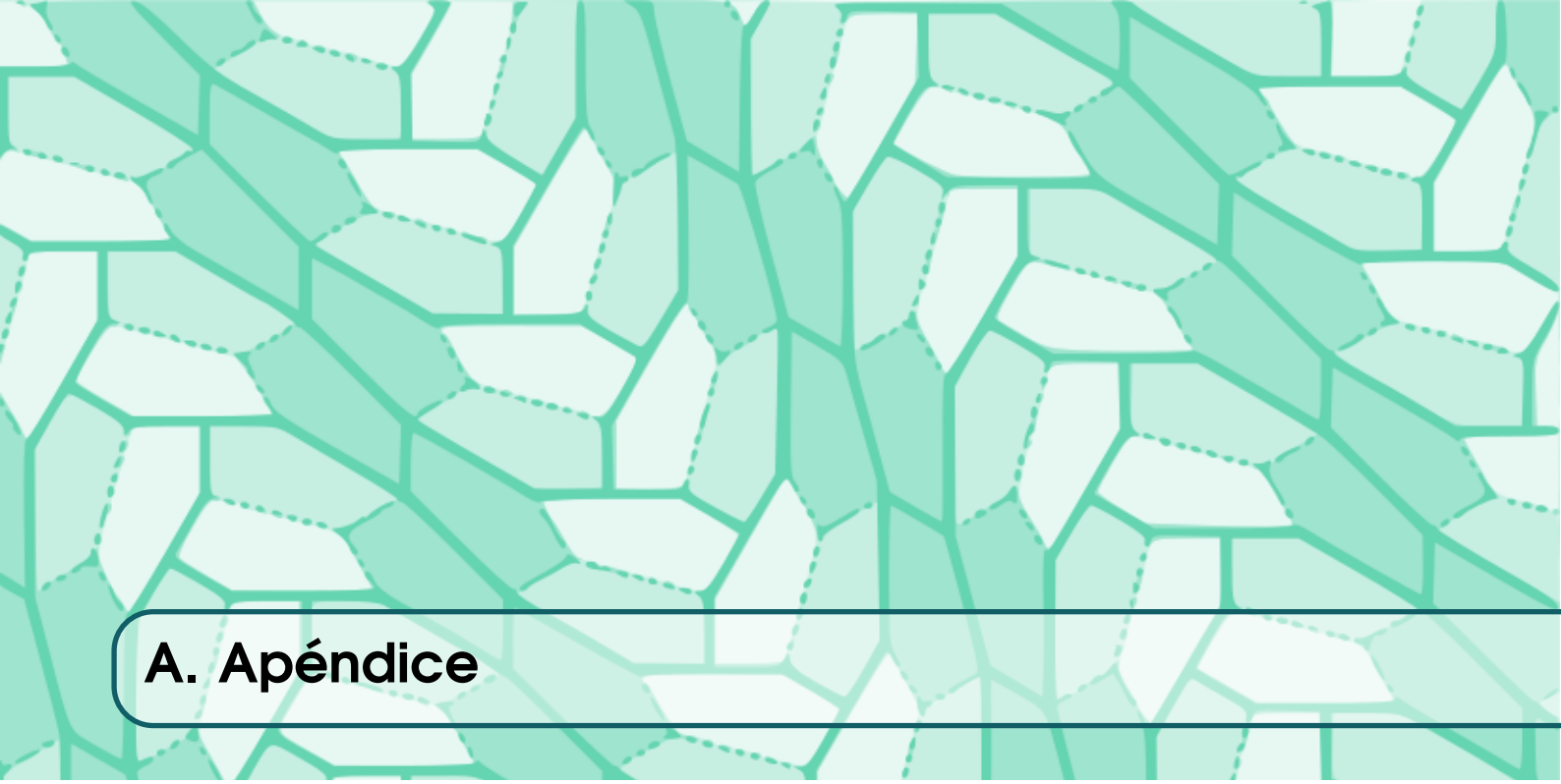
(VI) Hallar $\mathrm{car}(R_1)$ y $\#(R_1)$.

Ejercicio II.6.91 Probar que $\mathbb{R}[x,y]$ es un D.F.U. ¿es D.E.? ¿es D.I.P.?

Ejercicio II.6.92 Probar que $K[x,y]/(x^2 - y^3)$ es un dominio ¿Es D.F.U.?

Ejercicio II.6.93 En el anillo $\mathbb{C}[x,y]$ (ver Observación II.6.6) se pide:

(1) Probar que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x,y]$.
(2) Probar que $\mathbb{C}[x,y]/(x^2 + y^2 - 4)$ es un dominio.
(3) Si $I = (x^2 + y^2 - 4)$, probar que $(x + iy) + I \in U(\mathbb{C}[x,y]/I)$.



A. Apéndice

A.1 Número naturales. Principio de inducción

Los **Axiomas de Peano**, descritos a continuación, determinan de forma unívoca el conjunto de los números naturales:

(P0) 0 es un número natural.

(P1) Existe una aplicación del conjunto de los número naturales en sí mismo de modo que a cada número natural n se le asigna otro número natural $S(n)$ denominado **sucesor de** n.

(P2) La aplicación S es **inyectiva**, es decir, para todo para de números naturales n y m si se cumple que $S(n) = S(m)$, entonces se tiene que $n = m$.

(P3) No existe ningún número natural tal que $S(n) = 0$.

(P4) **(Axioma de inducción)** Si A es un subconjunto de los números naturales de forma que:

(I) $0 \in A$,

(II) para todo número natural n, si $n \in A$, entonces $S(n) \in A$,

entonces A es igual al conjunto de todos los números naturales.

Al conjunto que verifica estos axiomas lo denominamos **conjunto de los números naturales** y lo representamos por $\mathbb{N}$. Denotamos a sus elementos de la forma habitual $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$. En la versión original de Giuseppe Peano [17] de 1889 no incluyó al 0 como número natural, es decir, los axiomas se enunciaban sustituyendo 1 por 0, pero en el *Formulario mathematico* de 1908 [18] el propio G. Peano había cambiado de criterio presentando la versión que hemos descrito.

Veamos ahora algunas propiedades fundamentales del conjunto de los número naturales. Recordamos que una **proposición** es una sentencia declarativa que puede ser cierta o falsa. El axioma de inducción, convenientemente reformulado, se usa como método de demostración de proposiciones referidas a números naturales.

Imagen de cabecera: Teselación del plano mediante pentágonos convexos descubierta por Casey Mann, Jennifer McLoud y David Von Derau en 2015. En 2017, Michaël Rao demostró que con este último pentágono la lista de polígonos convexos que teselan el plano está completa.
(via https://www.gaussianos.com/michael-rao-termina-la-busqueda-de-poligonos-convexos-teseladores/)

Teorema A.1.1 (Principio de Inducción). Sea $P(n)$ una proposición definida para cada número natural $n \in \mathbb{N}$. Supongamos que:
(I) $P(0)$ es cierta.
(II) para todo $n \in \mathbb{N}$, si $P(n)$ es cierta entonces $P(S(n))$ también es cierta.
Entonces $P(n)$ es cierta para todo $n \in \mathbb{N}$.

Demostración. Consideramos el conjunto $A = \{n \in \mathbb{N} : P(n) \text{ es cierta}\}$. Por (I), tenemos que $0 \in A$. Dado $n \in \mathbb{N}$, si $n \in A$, por definición de A se tiene que $P(n)$ es cierta y, por (II), $P(S(n))$ también es cierta. En consecuencia, $S(n) \in A$ y por **(P4)**, concluimos que $A = \mathbb{N}$, es decir, $P(n)$ es cierta para todo $n \in \mathbb{N}$. ■

Empleando este resultado podemos definir la suma '$+$' en $\mathbb{N}$ de forma recursiva

(S0)	para cada	$n \in \mathbb{N}$	definimos	$n+0 := n,$
(S1)	para cada	$n,m \in \mathbb{N}$	definimos	$n+S(m) := S(n+m).$

El producto producto '$\cdot$' en $\mathbb{N}$ se define de forma recursiva a partir de la suma por

(M0)	para cada	$n \in \mathbb{N}$	definimos	$n \cdot 0 := 0,$
(M1)	para cada	$n,m \in \mathbb{N}$	definimos	$n \cdot S(m) := n \cdot m + n,$

y de la relación de orden habitual está dada por:

$$n \leq m \quad \Leftrightarrow \quad \text{existe} \quad k \in \mathbb{N} \quad \text{tal que} \quad n+k=m.$$

Empleando el teorema de recursión de Dedekind podemos probar que existe una única aplicación $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ que verifica los axiomas de la suma y lo mismo ocurre para el producto $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Mediante el Principio de Inducción, y de un modo directo pero laborioso, se puede probar que se satisfacen las propiedades clásicas conocidas (ver los Ejercicios de esta sección).

Por su importancia en el curso, veamos que el orden natural en $\mathbb{N}$ es un buen orden. Recordamos que dado un conjunto ordenado $(X, \leq)$ y $A \subseteq X$ un subconjunto no vacío, decimos que A tiene mínimo si existe $\alpha \in A$ tal que $\alpha \leq a$ para todo $a \in A$. En ese caso, escribimos $\alpha = \text{mín}(A)$. De un modo análogo se define el máximo.

Teorema A.1.2 (Principio de Buena Ordenación). Todo subconjunto no vacío de números naturales tiene mínimo.

Demostración. En primer lugar, definimos la proposición P para cada $n \in \mathbb{N}$ por

$$P(n)\text{: todo subconjunto no vacío de } \{0,1,2,\ldots,n\} \text{ tiene mínimo.}$$

Para $n = 0$, el único subconjunto no vacío de $\{0,1,2,\ldots,n\} = \{0\}$ es $\{0\}$ que tiene mínimo, luego $P(0)$ es cierta. Supongamos que $P(n)$ se cumple para un cierto $n \in \mathbb{N}$ y veamos que se cumple $P(n+1)$. Dado C un subconjunto no vacío de de $\{0,1,2,\ldots,n,n+1\}$, distinguimos dos casos:

(a) Si $C = \{n+1\}$, entonces $n+1 = \text{mín}(C)$.
(b) En otro caso, consideramos $D = C \cap \{0,1,\ldots,n\}$ que es un subconjunto no vacío de $\{0,1,\ldots,n\}$. Por hipótesis de inducción, $D = C \cap \{0,1,\ldots,n\}$ tiene mínimo que denotamos por $d = \text{mín}(D)$. Comprobamos de forma automática que $d = \text{mín}(C)$.

Por tanto, en ambos casos hemos probado que $P(n+1)$ es cierta. En consecuencia, por el Principio de Inducción (Teorema A.1.1), $P(n)$ es cierta para todo $n \in \mathbb{N}$.

Empleemos esta información para probar el teorema. Dado A un subconjunto de $\mathbb{N}$ no vacío, tomamos un elemento $k \in A$ lo que es posible porque A es no vacío. Consideramos $B := A \cap \{0,1,\dots,k\}$, observamos que B es un conjunto no vacío de $\{0,1,\dots,k\}$ porque $k \in B$. Por lo probado anteriormente B tiene un mínimo que denotamos por $b = \text{mín}(B)$. Comprobamos de forma directa que $b = \text{mín}(A)$. ■

El Axioma de Inducción y el Principio de Buena Ordenación están estrechamente relacionados pero no son equivalentes, para más información ver [16].
En determinadas situaciones puede resultar conveniente hacer uso de una versión diferente del Principio de Inducción.

Teorema A.1.3 (Principio de Inducción Completa). Sea $P(n)$ una proposición definida para cada número natural $n \in \mathbb{N}$. Supongamos que:
(I) $P(0)$ es cierta.
(II) para todo $n \in \mathbb{N}$, si $P(k)$ es cierta para todo $k < n+1$ entonces $P(n+1)$ también es cierta.
Entonces $P(n)$ es cierta para todo $n \in \mathbb{N}$.

Demostración. Directa porque las hipótesis de este enunciado son más fuertes que las del Principio de Inducción (Teorema A.1.1). ■

A partir de los naturales, existen diversas formas de construir los números enteros. Una posibilidad es considerar el conjunto de clases de equivalencia definidas en $\mathbb{N} \times \mathbb{N}$ por la relación

$$(n,m)R(k,\ell) \qquad \Leftrightarrow \qquad n+\ell = m+k.$$

La idea intuitiva es que la clase de un par $[(n,m)]_R$ representa el número entero obtenido como resultado de restar m a n. Por tanto, el conjunto de los números enteros es $\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/R$ y podemos extender la suma, el producto y el orden de $\mathbb{N}$ a $\mathbb{Z}$:

$$\begin{aligned} [(n,\, m)]_R + [(k,\ell)]_R &:= [(n+k,\, m+\ell)]_R, \\ [(n,\, m)]_R \cdot [(k,\, \ell)]_R &:= [(nk+m\ell,\, n\ell+mk)]_R, \\ [(n,\, m)]_R \leq [(k,\, \ell)]_R \quad &\Leftrightarrow \quad n+\ell \leq m+k. \end{aligned}$$

De este modo podemos considerar $\mathbb{N}$ como subconjunto de $\mathbb{Z}$ y de ahora en adelante denotaremos a sus elementos de la forma habitual:

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

y el subconjunto formado por los números naturales mayores o iguales que $k \in \mathbb{N}$ lo denotaremos por

$$\mathbb{N}_{\geq k} := \{k, k+1, k+2, k+3, k+4, \dots\}.$$

Observación A.1.4 Se puede probar una versión equivalente del Principio de Inducción para todo subconjunto de $\mathbb{Z}$ acotado inferiormente. En concreto si dado $m \in \mathbb{Z}$ suponemos que :
(I) $P(m)$ es cierta.
(II) para todo $n \in \mathbb{Z}$ con $n \geq m$, si $P(n)$ es cierta entonces $P(n+1)$ también es cierta.
Podemos concluir que $P(n)$ es cierta para todo $n \geq m$.

Haciendo las modificaciones pertinentes se puede obtener también una versión en $\mathbb{Z}$ del Principio de Inducción Completa.

Ejercicio A.1.5 Asumimos que $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ es una aplicación que satisface **(S0)** y **(S1)**. El objetivo de este ejercicio es probar que $(\mathbb{N}, +)$ es un monoide conmutativo haciendo uso del principio de inducción. Indicaciones:

(I) Probar que la suma es asociativa.
*Pista: para $n, m \in \mathbb{N}$ fijos aplicar **(P4)** a $SA_{n+m} = \{p \in \mathbb{N} : (n+m)+p = n+(m+p)\}$.*

(II) Probar que para todo $n \in \mathbb{N}$ se tiene que $n+0 = n = 0+n$.
*Pista: aplicar **(P4)** a $SC_0 = \{n \in \mathbb{N} : n = 0+n\}$.*

(III) Probar que para todo $n \in \mathbb{N}$ se tiene que $n+1 = 1+n$.
*Pista: aplicar **(P4)** a $SC_1 = \{n \in \mathbb{N} : n+1 = 1+n\}$.*

(IV) Probar que la suma es conmutativa.
*Pista: para $n \in \mathbb{N}$ fijo aplicar **(P4)** a $SC_n = \{m \in \mathbb{N} : n+m = m+n\}$.*

(V) Probar que para $n, m, p \in \mathbb{N}$ si $n+p = m+p$ entonces $n = m$ (Ley de cancelación).
Pista: ídem para $CS_{n,m} = \{p \in \mathbb{N} : \text{ si } n+p = m+p \text{ entonces } n = m\}$.

Ejercicio A.1.6 Asumimos que $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ es una aplicación que satisface **(M0)** y **(M1)**. Se pide:

(I) Probar las propiedad distributiva del producto respecto a la suma.
*Pista: para $n, m \in \mathbb{N}$ fijos aplicar **(P4)** a $D_{n+m} = \{p \in \mathbb{N} : (n+m)p = np+mp)\}$.*

(II) Probar el producto es asociativo.
*Pista: para $n, m \in \mathbb{N}$ fijos aplicar **(P4)** a $MA_{nm} = \{p \in \mathbb{N} : (nm)p = n(mp)\}$.*

(III) Probar que 1 es el elemento neutro, es decir, para todo $n \in \mathbb{N}$ se tiene que $n \cdot 1 = n = 1 \cdot n$
*Pista: aplicar **(P4)** a $MN_1 = \{n \in \mathbb{N} : n = 1 \cdot n\}$.*

(IV) Probar que el producto es conmutativo.
*Pista: para $n \in \mathbb{N}$ fijo aplicar **(P4)** a $MC_n = \{m \in \mathbb{N} : nm = mn\}$.*

(V) Probar que para $n, m, p \in \mathbb{N}$ si $n \cdot p = m \cdot p$ y $p \neq 0$ entonces $n = m$ (Ley de cancelación).

Ejercicio A.1.7 Probar que $(\mathbb{N}, \leq)$ es un conjunto ordenado. ¿Es una relación de orden total?

Ejercicio A.1.8 Probar que $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo y unitario. Indicaciones:

(I) Probar que la suma está bien definida (no depende de los representantes elegidos).
(II) Probar que la suma es conmutativa, asociativa, que tiene elemento neutro y opuesto.
(III) Probar que el producto está bien definido (no depende de los representantes elegidos).
(IV) Probar que se cumple la propiedad distributiva.
(V) Probar que el producto es asociativo, conmutativo y que tiene elemento neutro.
(VI) Probar que si dados $x, y \in \mathbb{Z}$ se tiene que $x \cdot y = 0$ entonces $x = 0$ o $y = 0$.
(VII) Probar que la ley de cancelación para el producto.
(VIII) Probar que la aplicación $i : \mathbb{N} \to \mathbb{Z}$ dada por $i(n) = [(n, 0)]_R$ es inyectiva y cumple que para todos $n, m \in \mathbb{N}$ se tiene que $i(n+m) = i(n) + i(m)$, $i(n \cdot m) = i(n) \cdot i(m)$, si $n \leq m$ entonces $i(n) \leq i(m)$.
(IX) Probar que la relación de orden es un orden total.

A.2 Divisibilidad en $\mathbb{Z}$

Gran parte de los resultado del Álgebra Abstracta se fundamentan en resultados elementales de los números enteros. En este apéndice se recogen las propiedades que son necesarias para el desarrollo teórico de la asignatura.

Definición A.2.1 Dados $a,b\in\mathbb{Z}$ decimos que a **divide a** b (o equivalentemente a **es divisor de** b o b **es múltiplo de** a) cuando existe $c\in\mathbb{Z}$ tal que $b=a\cdot c$. En el caso de que se verifique la propiedad escribimos $a\mid b$ y si no se satisface escribimos $a\nmid b$.

Observación A.2.2 Dados $a,b\in\mathbb{Z}$ tales que $a\mid b$ y $b\mid a$, entonces existen $c_1,c_2\in\mathbb{Z}$ de forma que $a=c_1\cdot b$ y que $b=c_2\cdot a$, luego $a=c_1b=c_1c_2a$. Observamos que

$$a-c_1c_2a=0 \quad\Rightarrow\quad (1-c_1c_2)a=0 \quad\Rightarrow\quad a=0 \text{ o } 1-c_1c_2=0.$$

Si $a=0$, entonces $b=c_1a=0$ y se cumple que $a=b$.
Si $1-c_1c_2=0$, entonces $1=c_1c_2$, como $c_1,c_2\in\mathbb{Z}$ tenemos que o $c_1=c_2=1$ o $c_1=c_2=-1$, en ambos caso se tiene que $a=\pm b$. En otras palabra, si $a\mid b$ y $b\mid a$, entonces $a=\pm b$.

En particular, hemos probado que

$$\forall n,m\in\mathbb{N} \quad \text{si} \quad m\mid n \quad \text{y} \quad m\mid n \quad\Rightarrow\quad m=n.$$

Teorema A.2.3 (División Euclídea). Sean $a,b\in\mathbb{Z}$ con $b\neq 0$. Entonces existen $q,r\in\mathbb{Z}$ únicos de forma que $a=bq+r$ con $0\leq r<|b|$.

Demostración. EXISTENCIA DEL COCIENTE Y EL RESTO
Consideramos el conjunto $R=\{a-bk : k\in\mathbb{Z} \text{ y } a-bk\in\mathbb{N}\}\subseteq\mathbb{N}$. Veamos que $R\neq\emptyset$.
Distinguimos tres casos: si $a\geq 0$, tomamos $k=0$ y vemos que $a\in R$; si $a<0$ y $b>0$, tomamos $k=a$ y $a-ab=a(1-b)\in R$; y si $a<0$ y $b<0$, tomamos $k=-a$ y $a+ab\in R$. En consecuencia, por el Principio de Buena Ordenación (Teorema A.1.2) existe el mínimo de R que denotamos por $r:=\min(R)\in\mathbb{N}$. Como $r\in R$, existe $k_0\in\mathbb{Z}$ tal que $a=bk_0+r$.
Tomamos $q:=k_0$ y veamos que $r<|b|$. Razonamos por reducción al absurdo, supongamos que $r\geq|b|$. En primer lugar, si $b>0$, entonces $|b|=b$ y $r-b\geq 0$ y $r-b=a-bq-b=a-b(q+1)$, luego $r-b\in R$ y $r-b<r$ lo que contradice que $r=\min(R)$. En segundo lugar si $b<0$, repetimos el procedimiento y vemos que $r+b\in R$ contradiciendo que $r=\min(R)$.

UNICIDAD DEL COCIENTE Y EL RESTO
Supongamos que existe $q_1,q_2,r_1,r_2\in\mathbb{Z}$ tales que $a=bq_1+r_1=bq_2+r_2$ con $0\leq r_1<|b|$ y $0\leq r_2<|b|$. En consecuencia, se cumple que $b(q_1-q_2)=r_2-r_1$. Si $q_1\neq q_2$, observamos que $|q_1-q_2|\neq 0$ y deducimos que

$$|b|\leq|b||q_1-q_2|=|r_2-r_1|\leq\max(r_1,r_2)<|b|,$$

lo que es imposible. Por consiguiente, necesariamente se tiene que $q_1=q_2$ y concluimos que $r_1=r_2$. ■

Observación A.2.4 La condición $0\leq r$ es esencial para garantizar la unicidad del cociente y el resto. Incluso imponiendo que $|r|<|b|$, no tenemos garantizada la unicidad. Por ejemplo, podemos dividir 14 entre 5 de dos formas diferentes de modo que $|r|<|b|$:

$$14=5(2)+4, \qquad 14=5(3)-1.$$

Definición A.2.5 Sean $a,b \in \mathbb{Z}$. Decimos que un elemento $d \in \mathbb{Z}$ es **un máximo común divisor de** a **y** b si
(MCD.I) se tiene que $d \mid a$ y $d \mid b$. (*Divisor común*)
(MCD.II) para todo $c \in \mathbb{Z}$ tal que $c \mid a$ y $c \mid b$ se cumple que $c \mid d$.
(*Máximo para la relación de divisibilidad*)

Definición A.2.6 Sean $a,b \in \mathbb{Z}$. Decimos que un elemento $m \in \mathbb{Z}$ es **un mínimo común múltiplo de** a **y** b si
(MCM.I) se tiene que $a \mid m$ y $b \mid m$. (*Múltiplo común*)
(MCM.II) para todo $n \in \mathbb{Z}$ tal que $a \mid n$ y $b \mid n$ se cumple que $m \mid n$.
(*Mínimo para la relación de divisibilidad*)

Proposición A.2.7 Sean $a,b \in \mathbb{Z}$ y $d,d',m,m' \in \mathbb{Z}$ tales que d y d' son dos máximos comunes divisores de a y b y m y m' son dos mínimos comunes múltiplos de a y b. Entonces se cumple que

$$d = \pm\, d' \qquad\qquad m = \pm\, m'.$$

Demostración. Como d satisface (MCD.I) se tiene que $d \mid a$ y $d \mid b$ y como d' satisface (MCD.II) tenemos que $d \mid d'$. De una manera análoga, se verifica que $d' \mid d$. En consecuencia, por la observación A.2.2, se tiene que $d = \pm d'$.

Análogamente, se prueba para el mínimo común múltiplo. ■

Notación A.2.8 Para evitar la dualidad de la proposición anterior diremos que:
(A) d es **el máximo común divisor de** a **y** b si d es un M.C.D. de a y b y si $\mathbf{d \geq 0}$ y escribiremos $d = \text{m.c.d.}\,(a,b)$.
(B) m es **el mínimo común múltiplo de** a **y** b si m es un M.C.M. de a y b y si $\mathbf{m \geq 0}$ y escribiremos $m = \text{m.c.m.}\,(a,b)$.

El siguiente teorema garantiza que máximo común divisor de dos números enteros cuales quiera siempre existe.

Teorema A.2.9 Sean $a,b \in \mathbb{Z}$. Existe $d \in \mathbb{N}$ tal que $d = \text{m.c.d.}\,(a,b)$ y existen $s,t \in \mathbb{Z}$ tales que $d = s \cdot a + t \cdot b$.

Demostración. Si $a = b = 0$, veamos que $0 = \text{m.c.d.}\,(a,b)$. Observamos que $0 \mid a$ y $0 \mid b$ porque $a = 0 = 0 \cdot 1$ y $b = 0 = 0 \cdot 1$, luego 0 cumple (MCD.I). Dado $c \in \mathbb{Z}$ tal que $c \mid a$ y $c \mid b$, siempre se cumple trivialmente que $c \mid 0$, luego 0 cumple (MCD.II). Como $0 \in \mathbb{N}$, concluimos que $0 = \text{m.c.d.}\,(0,0)$. Basta tomar $0 = 0 \cdot 0 + 0 \cdot 0$.
Si $a \neq 0$ o $b \neq 0$, consideramos el conjunto

$$D = \{s \cdot a + t \cdot b \,:\, s,t \in \mathbb{Z} \text{ y } s \cdot a + t \cdot b \in \mathbb{N}_{\geq 1}\}.$$

Como $a \neq 0$ o $b \neq 0$, tenemos que $D \neq \emptyset$ porque tomando $s = a$ y $t = b$ tenemos que $a^2 + b^2 > 0$. Por el Principio de Buena Ordenación (Teorema A.1.2), D tiene un mínimo que denotamo por $d := \text{mín}(D)$. Veamos que $d = \text{m.c.d.}\,(a,b)$. Haciendo la división euclídea de a entre d (Teorema A.2.3), vemos que existen $q,r \in \mathbb{Z}$ con $0 \leq r < d$ tales que $a = qd + r$. Razonando por reducción al absurdo supongamos que $r > 0$. Como $r = a - qd$ y $d = s_0 a + t_0 b$ porque $d \in D$, tenemos que

$$r = a - qd = a - q(s_0 a + t_0 b) = (1 - s_0 q)a + (-q t_0)b.$$

Como $r > 0$, se deduce que $r \in D$ lo que es imposible porque sabíamos que $r < d$ y que $d = \text{mín}(D)$. Por tanto, necesariamente $r = 0$ y deducimos que $d \mid a$. Análogamente se prueba que $d \mid b$, es decir, se verifica (MCD.I).

Veamos que se cumple (MCD.II). Dado $c \in \mathbb{Z}$ tal que $c \mid a$ y $c \mid b$, entonces existen $k, \ell \in \mathbb{Z}$ tales que $a = kc$ y $b = \ell c$. Como $d \in D$, $d = s_0 a + t_0 b$ y vemos que

$$d = s_0 a + t_0 b = s_0 kc + t_0 \ell c = (s_0 k + t_0 \ell)c.$$

En consecuencia, concluimos que $c \mid d$. Como d verifica (MCD.I) y (MCD.II) y $d \in \mathbb{N}_{\geq 1}$, se cumple que $d = \text{m.c.d.}\,(a,b)$. ■

De la demostración del teorema anterior deducimos la siguiente propiedad fundamental.

Corolario A.2.10 (Identidad de Bezout) Sean $a, b \in \mathbb{Z}$ y $d = \text{m.c.d.}\,(a,b)$. Entonces existen $s,t \in \mathbb{Z}$ tales que

$$s \cdot a + t \cdot b = d.$$

Recíprocamente, si dado $c \in \mathbb{Z}$ existen $\tilde{s}, \tilde{t} \in \mathbb{Z}$ tales que

$$\tilde{s} \cdot a + \tilde{t} \cdot b = c,$$

entonces $\text{m.c.d.}\,(a,b) \mid c$.

Demostración. La primera afirmación está demostrada en el teorema anterior.
Por otra parte, dado $c \in \mathbb{N}_{\geq 1}$ de forma que existen $\tilde{s}, \tilde{t} \in \mathbb{Z}$ tales que $\tilde{s} \cdot a + \tilde{t} \cdot b = c$, tenemos que $c \in D = \{s \cdot a + t \cdot b \,:\, s,t \in \mathbb{Z} \text{ y } s \cdot a + t \cdot b \in \mathbb{N}_{\geq 1}\}$. Haciendo la división euclídea de c entre d (Teorema A.2.3), vemos que existen $q, r \in \mathbb{Z}$ con $0 \leq r < d$ tales que $c = qd + r$. Razonando por reducción al absurdo supongamos que $r > 0$. Como $r = c - qd$ y $d = sa + tb$ porque $d \in D$, tenemos que

$$r = c - qd = \tilde{s} \cdot a + \tilde{t} \cdot b - q(sa + tb) = (\tilde{s} - sq)a + (\tilde{t} - qt)b.$$

Como $r > 0$, se deduce que $r \in D$ lo que es imposible porque sabíamos que $r < d$ y que $d = \text{mín}(D)$. Por tanto, necesariamente $r = 0$ y deducimos que $d \mid c$. ■

Observación A.2.11 En particular si dados $a, b \in \mathbb{Z}$ existen $s,t \in \mathbb{Z}$ tales que $sa + tb = 1$, deducimos que $\text{m.c.d.}\,(a,b) \mid 1$, luego $\text{m.c.d.}\,(a,b) = 1$.

De una forma similar se puede probar la existencia del mínimo común múltiplo de dos número enteros cualesquiera y obtener algunas propiedades clásicas.

Teorema A.2.12 Sean $a, b \in \mathbb{Z}$. Existe $m \in \mathbb{N}$ tal que $m = \text{m.c.m.}\,(a,b)$.

Corolario A.2.13 Sean $a, b, c \in \mathbb{Z}$. Entonces se cumple que

(I) $\text{m.c.d.}\,(a,b) \cdot \text{m.c.m.}\,(a,b) = |a \cdot b|$.
(II) $\text{m.c.d.}\,(ac, ab) = |a| \text{m.c.d.}\,(c,b)$.
(III) Si $d = \text{m.c.d.}\,(a,b)$, $a = d \cdot a_0$ y $b = d \cdot b_0$, entonces $\text{m.c.d.}\,(a_0, b_0) = 1$.
(IV) Si $a \mid bc$ y $\text{m.c.d.}\,(a,b) = 1$, entonces $a \mid c$.
(V) Si $\text{m.c.d.}\,(a,b) = \text{m.c.d.}\,(a,c) = 1$, entonces $\text{m.c.d.}\,(a,bc) = 1$.
(VI) Si $\text{m.c.d.}\,(a,b) = 1$, entonces $\text{m.c.d.}\,(a+b, a-b) \in \{1,2\}$.
(VII) $\text{m.c.d.}\,(\text{m.c.d.}\,(a,b),\, c) = \text{m.c.d.}\,(a,\, \text{m.c.d.}\,(b,c))$.
(VIII) $\text{m.c.d.}\,(a, \text{m.c.m.}\,(b,c)) = \text{m.c.m.}\,(\text{m.c.d.}\,(a,b), \text{m.c.d.}\,(a,c))$.

Observación A.2.14 Por el CorolarioA.2.13.(VII), podemos definir de forma recursiva el máximo común divisor de un conjunto finito de números. Para cada $n \in \mathbb{N}_{\geq 1}$, $n \geq 2$, dados $a_1, a_2, \ldots, a_{n-1}, a_n \in \mathbb{Z}$ definimos

$$\text{m.c.d.}\,(a_1, a_2, \ldots, a_{n-1}, a_n) := \text{m.c.d.}\,(\text{m.c.d.}\,(a_1, a_2, \ldots, a_{n-1}), a_n).$$

De una forma análoga, se define el $\text{m.c.m.}\,(a_1, a_2, \ldots, a_{n-1}, a_n)$.

Adicionalmente, gracias a la división euclídea disponemos de un algoritmo que nos permite calcular un máximo común divisor de dos elementos, sin necesidad de conocer su factorización en irreducibles: **el Algoritmo de Euclides**. La siguiente proposición garantiza que el algoritmo finaliza con éxito.

Proposición A.2.15 Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Si $q, r \in \mathbb{Z}$ son los elementos dados por el Teorema A.2.3, es decir, tales que $a = bq + r$ con $0 \leq r < |b|$, entonces tenemos que

$$\text{m.c.d.}\,(a, b) = \text{m.c.d.}\,(b, r).$$

Demostración. Escribimos $d = \text{m.c.d.}\,(a, b)$ y $d' = \text{m.c.d.}\,(b, r)$, veamos que $d \mid d'$ y que $d' \mid d$. Por la identidad de Bézout sabemos que existen $s, t \in \mathbb{Z}$ tales que $sa + tb = d$, sustituyendo $a = bq + r$, tenemos que $s(bq + r) + tb = d$. Por tanto, se cumple que $sr + (qs + t)b = d$, luego d es un múltiplo de $d' = \text{m.c.d.}\,(b, r)$.

Análogamente, por la identidad de Bézout, sabemos que existen $s', t' \in \mathbb{Z}$ tales que $s'b + t'r = d'$, luego $(s' - t'q)b + t'a = d'$ y tenemos que d' es múltiplo de $d = \text{m.c.d.}\,(a, b)$. ■

Establecemos el siguiente algoritmo.

ALGORITMO DE EUCLIDES

Entrada: Enteros $a, b \in \mathbb{Z}$ con $b \neq 0$.

Salida: $\text{m.c.d.}\,(a, b)$.

1. $r_0 := a$ y $r_1 := b$.
2. $i \leftarrow 1$.
3. Mientras $r_i \neq 0$ hacer:
   - **3.1.** Dividir r_{i-1} entre r_i para obtener q_i y r_{i+1} con $r_{i-1} = r_i q_i + r_{i+1}$.
   - **3.2.** $i \leftarrow i + 1$.
4. La salida es: $|r_{i-1}|$.

Como cada vez que aplicamos el paso **3.1** tenemos que o bien $|r_{i+1}| < |r_i|$ o bien $r_{i+1} = 0$ podemos asegurar existe un $n \in \mathbb{N}_{\geq 1}$ de modo que el algoritmo termina en n iteraciones. Hemos visto que $\text{m.c.d.}\,(m, 0) = |m|$, luego cuando el algoritmo termina, se cumple que $r_n = 0$, luego $\text{m.c.d.}\,(r_{n-1}, r_n) = |r_{n-1}|$. Gracias a la Proposición A.2.15, sabemos que

$$\text{m.c.d.}\,(a, b) = \text{m.c.d.}\,(r_0, r_1) = \text{m.c.d.}\,(r_1, r_2) = \cdots = \text{m.c.d.}\,(r_{n-2}, r_{n-1}) = \text{m.c.d.}\,(r_{n-1}, r_n) = |r_{n-1}|.$$

En otras palabras, el Algoritmo de Euclides finaliza de forma correcta y el **último resto no nulo** r_{n-1} es el máximo común divisor de a y b.

Una ligera modificación del algoritmo, nos permite obtener elementos s,t del dominio, de modo que se satisface la **Identidad de Bezout** (ver Corolario A.2.10), es decir, tales que $d = as+bt$.

ALGORITMO DE EUCLIDES EXTENDIDO

Entrada: Enteros $a,b \in \mathbb{Z}$ con $b \neq 0$.

Salida: Un máximo común divisor d de a y b y elementos $s,t \in \mathbb{Z}$ tales que $d = as+bt$.

1. $r_0 := a$, $r_1 := b$, $s_0 := 1$, $t_0 := 0$, $s_1 := 0$, $t_1 := 1$.

2. $i \leftarrow 1$.

3. Mientras $r_i \neq 0$ hacer:

3.1. Dividir r_{i-1} entre r_i para obtener q_i, r_{i+1} con $r_{i-1} = r_i q_i + r_{i+1}$.

3.2. $s_{i+1} := s_{i-1} - q_i s_i$.

3.3. $t_{i+1} := t_{i-1} - q_i t_i$.

3.4. $i \leftarrow i+1$.

4. La salida es: r_{i-1} que es un máximo común divisor de a y b que se escribe como $r_{i-1} = a s_{i-1} + b t_{i-1}$.

Ejemplo A.2.16 Queremos calcular el máximo común divisor y los enteros de la identidad de Bezout para $a = 13544$ y $b = 2164$ en $\mathbb{Z}$.

En este caso, de acuerdo con la notación que del algoritmo de euclides $r_0 := a$, $r_1 := b$, $s_0 := 1$, $t_0 := 0$, $s_1 := 0$, $t_1 := 1$, lo que podemos escribir como:

$$\begin{aligned} (r_0 = r_0 s_0 + r_1 t_0) \qquad & 13544 = 13544 \cdot (1) + 2164 \cdot (0), \\ (r_1 = r_0 s_1 + r_1 t_1) \qquad & 2164 = 13544 \cdot (0) + 2164 \cdot (1). \end{aligned}$$

Como el cociente de dividir $r_0 = 13544$ entre $r_1 = 2164$ es $q_1 = 6$ multiplicando la segunda fila por -6 y sumando el resultado a la primera obtenemos r_2, t_2, s_2 a la vez, es decir, se tiene que

$$\begin{aligned} (r_0 = r_0 s_0 + r_1 t_0) \qquad & 13544 = 13544 \cdot (1) + 2164 \cdot (0), \\ (r_1 = r_0 s_1 + r_1 t_1) \qquad & 2164 = 13544 \cdot (0) + 2164 \cdot (1), \\ (r_2 = r_0 s_2 + r_1 t_2) \qquad & 560 = 13544 \cdot (1) + 2164 \cdot (-6). \end{aligned}$$

Repitiendo el procedimiento con la segunda y la tercera línea, es decir, dividiendo $r_1 = 2164$ entre $r_2 = 560$, el cociente es $q_2 = 3$. Multiplicando por -3 la tercera línea y sumándole la segunda vemos que

$$\begin{aligned} (r_0 = r_0 s_0 + r_1 t_0) \qquad & 13544 = 13544 \cdot (1) + 2164 \cdot (0), \\ (r_1 = r_0 s_1 + r_1 t_1) \qquad & 2164 = 13544 \cdot (0) + 2164 \cdot (1), \\ (r_2 = r_0 s_2 + r_1 t_2) \qquad & 560 = 13544 \cdot (1) + 2164 \cdot (-6), \\ (r_3 = r_0 s_3 + r_1 t_3) \qquad & 484 = 13544 \cdot (-3) + 2164 \cdot (19). \end{aligned}$$

Operamos de este modo hasta obtener un resto nulo:

$$
\begin{aligned}
(r_0 = r_0s_0 + r_1t_0) \quad & 13544 = 13544 \cdot (1) + 2164 \cdot (0),\\
(r_1 = r_0s_1 + r_1t_1) \quad & 2164 = 13544 \cdot (0) + 2164 \cdot (1),\\
(r_2 = r_0s_2 + r_1t_2) \quad & 560 = 13544 \cdot (1) + 2164 \cdot (-6),\\
(r_3 = r_0s_3 + r_1t_3) \quad & 484 = 13544 \cdot (-3) + 2164 \cdot (19),\\
(r_4 = r_0s_4 + r_1t_4) \quad & 76 = 13544 \cdot (4) + 2164 \cdot (-25),\\
(r_5 = r_0s_5 + r_1t_5) \quad & 28 = 13544 \cdot (-27) + 2164 \cdot (169),\\
(r_6 = r_0s_6 + r_1t_6) \quad & 20 = 13544 \cdot (58) + 2164 \cdot (-363),\\
(r_7 = r_0s_7 + r_1t_7) \quad & 8 = 13544 \cdot (-85) + 2164 \cdot (532),\\
(r_8 = r_0s_8 + r_1t_8) \quad & 4 = 13544 \cdot (228) + 2164 \cdot (-1427),\\
(r_9 = r_0s_9 + r_1t_9) \quad & 0 = 13544 \cdot (-541) + 2164 \cdot (3386).
\end{aligned}
$$

En la penúltima línea, la correspondiente al último resto no nulo, se encuentran el valor del m.c.d y la igualdad de Bezout buscados. En otras palabras, $d = 4$, $s = 228$ y $t = -1427$.

Definición A.2.17 Dado $p \in \mathbb{Z}\backslash\{-1,0,1\}$ decimos que p **es primo (en** $\mathbb{Z}$**)** si para todos $a,b \in \mathbb{Z}$ tales que $p \mid ab$, entonces $p \mid a$ o $p \mid b$.

Observación A.2.18 Empleando la definición, podemos probar por inducción que si $p \in \mathbb{Z}$ es primo, para todos $a_1a_2\cdots a_n \in \mathbb{Z}$ tales que $p \mid a_1a_2\cdots a_n$, entonces $p \mid a_i$ para algún $i \in \{1,\ldots,n\}$.

Observación A.2.19 1 no es primo, para más información se recomienda leer [2, 3].

Proposición A.2.20 Dado $p \in \mathbb{Z}\backslash\{-1,0,1\}$ tenemos que

p es primo si y solo si sus únicos divisores son ± 1 y $\pm p$.

Demostración. En primer lugar, supongamos que p es primo y veamos que sus únicos divisores son ± 1 y $\pm p$. Dado $a \in \mathbb{Z}$ tal que $a \mid p$ existe $b \in \mathbb{Z}$ con $p = ab$. Por tanto, tenemos que $p \mid ab$ y como p es primo $p \mid a$ o $p \mid b$. Si $p \mid a$ como $a \mid p$, por la Observación A.2.2, tenemos que $a = \pm p$. Supongamos que $p \mid b$, luego existe $r \in \mathbb{Z}$ tal que $pr = b$. Por consiguiente, $p = ab = arp$ y vemos que $p(1-ar) = 0$. Como $p \neq 0$, se tiene que $1 = ar$ y, en consecuencia, $a = \pm 1$.

Recíprocamente, supongamos que los únicos divisores de p son ± 1 y $\pm p$. Dados $a,b \in \mathbb{Z}$ tales que $p \mid ab$, supongamos que $p \nmid a$ y veamos que $p \mid b$. Como $p \nmid a$, $-p \nmid a$ y de entre los divisores de p, que por hipótesis son ± 1 y $\pm p$, los únicos que son divisores de a son ± 1. En consecuencia, se tiene que m.c.d.$(p,a) = 1$ y por la Identidad de Bezout existen $s,t \in \mathbb{Z}$ tales que $ps + at = 1$. Multiplicando por b a ambos lados tenemos que $psb + abt = b$, como $p \mid psb$ y $p \mid abt$ porque $p \mid ab$ deducimos que $p \mid (psb + abt)$ y concluimos que $p \mid b$. Por consiguiente, p es primo. ■

La importancia de los números primos se manifiesta en el siguiente teorema.

Teorema A.2.21 (Teorema fundamental de la Aritmética). Todo $n \in \mathbb{N}_{\geq 2}$ se puede escribir de forma única como

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$$

donde $0 < p_1 < p_2 < \cdots < p_k$ son primos y $n_i \in \mathbb{N}_{\geq 1}$.

Demostración. EXISTENCIA

Emplearemos el Principio de Inducción Completa que se cumple la existencia. Para $n = 2$, se cumple porque 2 es primo. Supongamos que se cumple el teorema para todos los $k \in \mathbb{N}_{\geq 2}$ y menores que un cierto n. Si n es primo, hemos terminado. Si n no es primo, por la Proposición A.2.20, existe $a \in \mathbb{Z}$ con $1 < a < n$ tal que $a \mid n$, es decir, $n = ab$ con $a, b \in \{2, \ldots, n-1\}$. Por hipótesis de inducción, $a = q_1^{m_1} q_2^{m_2} \cdots q_k^{m_k}$ y $b = q_{k+1}^{m_{k+1}} q_{k+2}^{m_{k+2}} \cdots q_\ell^{m_\ell}$ con $0 < q_1 < q_2 < \cdots < q_k$ y $0 < q_{k+1} < q_{k+2} < \cdots < q_\ell$ primos. En consecuencia, reorganizando los factores primos que son iguales

$$n = ab = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}.$$

donde $0 < p_1 < p_2 < \cdots < p_k$ son primos y $n_i \in \mathbb{N}_{\geq 1}$. Por consiguiente, por el Principio de Inducción Completa queda demostrada la existencia.

UNICIDAD

Para $n = 2$, se verifica la unicidad. Razonamos por reducción al absurdo, supongamos que existe un número natural mayor que dos que admite dos descomposiciones distintas en factores primos. Empleando el Principio de Buena Ordenación, elegimos $n \in \mathbb{N}_{\geq 3}$ el menor natural que cumple que

$$n = q_1^{m_1} q_2^{m_2} \cdots q_\ell^{m_\ell} = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

con $0 < q_1 < q_2 < \cdots < q_\ell$ y $0 < p_1 < p_2 < \cdots < p_k$ primos y $n_i, m_i \in \mathbb{N}_{\geq 1}$ y deforma que las dos descomposiciones no son iguales. Como $p_1 \mid n$, por la definición de número primo $p_1 \mid q_i$ para algún i. Como q_i y p_1 son primos, $p_1 = q_i$. Cancelando los correspondientes factores en la descomposición de n, vemos que

$$q_1^{m_1} q_2^{m_2} \cdots q_i^{m_i - 1} \cdots q_\ell^{m_\ell} = p_1^{n_1 - 1} p_2^{n_2} \cdots p_k^{n_k}$$

En consecuencia, hemos obtenido dos factorizaciones distintas (porque $p_1 = q_i$) de un número natural más pequeño que n, contradiciendo que n era el más pequeño, con dos descomposiciones. ■

Este resultado se extiende a todos los enteros negativos menores o iguales que -2, realizando las modificaciones oportunas. Gracias al Teorema Fundamental de la Aritmética podemos escribir el máximo común divisor y el mínimo común múltiplo de dos enteros a, b en términos de su descomposición en números primos.

Corolario A.2.22 Sean $a, b \in \mathbb{N}_{\geq 2}$. Por el Teorema Fundamental de la Aritmética, podemos afirmar que

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \qquad \text{y} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n},$$

con $p_i \in \mathbb{N}_{\geq 1}$ primo y con $\alpha_i, \beta_i \in \mathbb{N}$ ($\alpha_i = 0$ si p_i no es factor de a y $\beta_i = 0$ si p_i no es factor de a). Para todo $i \in \{1, 2, \ldots, n\}$ definimos $\delta_i := \min(\alpha_i, \beta_i)$ y $\mu_i := \max(\alpha_i, \beta_i)$, entonces se cumple que

$$\text{m.c.d.}\,(a, b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n} \quad \text{y} \quad \text{m.c.m.}\,(a, b) = p_1^{\mu_1} p_2^{\mu_2} \cdots p_n^{\mu_n}.$$

Observamos que recuperamos la definición usual: el máximo común divisor son los factores comunes elevados al mínimo exponente (si no son comunes $\delta_i = 0$) y el mínimo común múltiplo son los factores comunes y no comunes elevados al máximo exponente.

Ejercicio A.2.23 De acuerdo con la Definición A.2.5. Determinar dos máximos comunes divisores diferentes de 36 y 24 en $\mathbb{Z}$.

Ejercicio A.2.24 Dado $m \in \mathbb{Z}$, calcular m.c.d.$(0,m)$ y m.c.m.$(0,m)$

Ejercicio A.2.25 Probar el Teorema A.2.12 y el Corolario A.2.13.

Ejercicio A.2.26 (Construcción de $\mathbb{Q}$). Partimos del anillo $(\mathbb{Z},+,\cdot)$ y definimos sobre $A = \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ la relación de equivalencia

$$(p,q)R(p',q') \quad \Leftrightarrow \quad p \cdot q' = q \cdot p.$$

Definimos $\mathbb{Q} := A/R$ y se definen las leyes internas en $\mathbb{Q}$ por

$$[(p_1,q_1)]_R + [(p_2,q_2)]_R := [(p_1 \cdot q_2 + p_2 \cdot q_1, q_1 \cdot q_2)]_R.$$
$$[(p_1,q_1)]_R \cdot [(p_2,q_2)]_R := [(p_1 \cdot p_2, q_1 \cdot q_2)]_R.$$

Demostrar que ambas leyes internas están bien definidas y que dotan a $\mathbb{Q}$ de estructura de cuerpo.

Ejercicio A.2.27 (Lenguaje de congruencias). Sean x,y dos enteros y $n \in \mathbb{N}_{\geq 1}$ dice que x **es congruente con** y **módulo** n, si $n|(x-y)$, es decir, si $x - y = kn$ para algún $k \in \mathbb{Z}$. En este caso escribimos $x \equiv y\,(\text{mód}\,n)$.
Sobre $\mathbb{Z}$ se define la siguiente relación

$$x \sim_n y \qquad \Leftrightarrow \qquad x \equiv y\,(\text{mód}\,n).$$

Se pide:

(I) Probar que $\sim_n$ es una relación de equivalencia.
(**la relación de congruencia módulo** n)

(II) Para cada $a \in \mathbb{Z}$, denotamos por $[a]_n$ a la clase de a en $\mathbb{Z}/\sim_n$. Probar que $\mathbb{Z}/n\mathbb{Z} = \{0,1,\ldots,n-1\}$ es un sistema completo de representantes de $\mathbb{Z}/\sim_n$.

(III) Si $a \equiv a'\,(\text{mód}\,n)$ y $b \equiv b'\,(\text{mód}\,n)$, probar que

$$a + b \equiv a' + b'\,(\text{mód}\,n)$$

$$a \cdot b \equiv a' \cdot b'\,(\text{mód}\,n)$$

Deducir que en $\mathbb{Z}/\sim_n$, para $[a]_n, [b]_n \in \mathbb{Z}/\sim_n$ si se define la suma y el producto como

$$[a]_n + [b]_n := [a+b]_n,$$

$$[a]_n \bullet [b]_n := [a \cdot b]_n,$$

las operaciones están bien definidas.

(IV) Dados $r,s \in \mathbb{Z}/n\mathbb{Z}$. Si $+$ y $\bullet$ son la operaciones definidas en el Ejercicio I.1.6 en $\mathbb{Z}/n\mathbb{Z}$, probar que:

$$[r]_n + [s]_n = [r+s]_n,$$
$$[r]_n \bullet [s]_n = [r \bullet s]_n.$$

Concluir, empleando dicho ejercicio, que $(\mathbb{Z}/\sim_n, +)$ es un grupo abeliano y que $(\mathbb{Z}/\sim_n, \bullet)$ es un monoide conmutativo.

Ejercicio A.2.28 (Función de Euler). Para cada número natural n, se define la función de Euler $\varphi(n)$ como el número de enteros positivos menores que n relativamente primos con n, es decir:

$$\varphi(n) = \#\{x \in \mathbb{N} \quad : \quad x < n \quad \text{y} \quad \text{m.c.d.}\,(x,n) = 1\},$$

donde $\#A$ es el cardinal o número de elementos del conjunto A. Para los primeros números naturales, la función de Euler es:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Probar que:

(I) Si p es primo y $\alpha \in \mathbb{N}_{\geq 1}$, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

(II) Si $m.c.d(m,n) = 1$, entonces $\varphi(m \cdot n) = \varphi(m)\varphi(n)$.

(III) Concluir que si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, con cada p_j primo y distintos dos a dos, entonces

$$\varphi(n) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right).$$

Ejercicio A.2.29 (Ecuaciones Diofánticas Lineales). Sean $a, b \in \mathbb{Z}$ y d su máximo común divisor. Se pide:

(I) Probar que la ecuación diofántica

$$a \cdot x + b \cdot y = c,$$

tiene solución $(x,y) \in \mathbb{Z}^2$ si y solo si $d \mid c$.

(II) Escribimos $a = d \cdot a_0$ y $b = d \cdot b_0$ y consideramos los enteros de la Identidad de Bezout $s,t \in \mathbb{Z}$ tales que

$$s \cdot a + t \cdot b = d.$$

En caso de que la ecuación diofántica tenga solución, es decir, si $c = dc_0$, probar que $(x,y) \in \mathbb{Z}^2$ es solución de $a \cdot x + b \cdot y = c$ si y solo si es de la forma

$$\begin{cases} x = s\, c_0 - r\, b_0, \\ y = t\, c_0 + r\, a_0. \end{cases}$$

para algún $r \in \mathbb{Z}$.

Ejercicio A.2.30 Cinco hombres naufragaron en una isla. Pasaron el primer día recogiendo cocos. Deciden que, como está oscureciendo, esperarán hasta el día siguiente para repartirlos. Durante la noche, un hombre se despertó y decidió llevarse su parte de los cocos. Los repartió en cinco montones. Le sobró un coco, así que se lo dio al mono, luego escondió su parte, juntó las otras cuatro partes en un montón y se volvió a dormir. Pasado un rato se despertó un segundo hombre e hizo lo mismo. Después de dividir los cocos en cinco montones, sobró un coco que le dio al mono. Luego escondió su parte, juntó el resto y volvió a acostarse. El tercer, cuarto y quinto hombre siguieron exactamente el mismo procedimiento. A la mañana siguiente, tras despertarse todos, dividieron los cocos restantes en cinco partes iguales. Esta vez no sobró ningún coco. ¿Cuál es el menor número de cocos que puede haber en el montón original?¿y si al repartirlos cocos por la mañana sobra un coco?

Ejercicio A.2.31 Resolver las siguientes **ecuaciones diofánticas**:

$$\text{(I)}\ 6x+8y=10 \qquad \text{(II)}\ 2023x+51y=190 \qquad \text{(III)}\ 45815x+15400y=385.$$

Ejercicio A.2.32 (Inversos en $U(\mathbb{Z}/n\mathbb{Z})$). En el Ejercicio I.1.7 se ha probado que para $n\in\mathbb{N}_{\geq 2}$ se tiene que $a\in\mathbb{Z}/n\mathbb{Z}$ tiene inverso para el producto, es decir, $a\in U(\mathbb{Z}/n\mathbb{Z})$ si y solo si m.c.d.$(a,n)=1$. La demostración es constructiva y nos permite obtener el siguiente algoritmo para calcular el inverso de a módulo n.

> **ALGORITMO CÁLCULO DEL INVERSO EN $U(\mathbb{Z}/n\mathbb{Z})$**
>
> **Entrada:** Elementos $a\in\mathbb{Z}/n\mathbb{Z}$ y $n\in\mathbb{N}_{\geq 2}$.
>
> **Salida:** O bien 'No existe' o bien $b\in\mathbb{Z}/n\mathbb{Z}$ tal que $ab\equiv 1 \mod n$.
>
> 1. Aplicar el Algoritmo de Euclides para calcular $s,t\in\mathbb{Z}$ y $d=\text{m.c.d.}(a,n)\in\mathbb{N}$ tal que $as+nt=d$.
> 2. Si $d\neq 1$, la salida es: 'No existe'.
> 3. Si $d=1$, la salida es: $s \mod n$.

Determinar si a tiene inverso para el producto en $\mathbb{Z}/n\mathbb{Z}$ y, en caso de existir, calcularlo:

$$\text{(I)}\ a=37,\ n=73 \qquad \text{(II)}\ a=81,\ n=1521 \qquad \text{(III)}\ a=1521,\ n=2023.$$

Ejercicio A.2.33 Podemos emplear la estructura de grupo de $U(\mathbb{Z}/n\mathbb{Z})$ para calcular potencias de números módulo n. Demostrar los siguientes resultados:

(I) **[Teorema de Euler]** Si $a\in\mathbb{Z}$ y $n\in\mathbb{N}_{\geq 2}$ son tales que $m.c.d(a,n)=1$, entonces

$$a^{\varphi(n)}\equiv 1\,(\text{mód } n).$$

(ver Ejercicio A.2.27 y Ejercicio A.2.28 para la notación).

(II) **[Pequeño Teorema de Fermat]** Si p es primo y no es divisor $a\in\mathbb{Z}$, entonces

$$a^{p-1}\equiv 1\,(\text{mód } p).$$

(Nota: Estos resultados se pueden demostrar empleando técnicas elementales de aritmética modular, pero también es posible demostrarlos de forma sencilla con el Corolario I.5.13)
Emplear los teoremas anteriores para calcular la clase de las siguientes potencias:

$$\text{(I)}\ 2024^{2024}\,(\text{mód } 13) \quad \text{(II)}\ 625^{512}\,(\text{mód } 72) \quad \text{(III)}\ 11^{954}\,(\text{mód } 20); \quad \text{(IV)}\ 5^{17^{17}}\,(\text{mód } 9).$$

Calcular $2^{70}+3^{30}(\text{mód } 17)$.
Calcular el último dígito decimal del 3^{400}.

Ejercicio A.2.34 (Teorema chino del resto). Sean $a,b\in\mathbb{Z}$ y $m,n\in\mathbb{N}$ no nulos y primos entre sí. Demostrar que el sistema de ecuaciones

$$\begin{cases} x \equiv a & (\text{mód } m) \\ x \equiv b & (\text{mód } n) \end{cases}$$

tiene una única solución módulo $m\cdot n$. Obtener un algoritmo para calcular x en función de a,b,n y m. ¿Qué ocurre si m,n no son primos entre sí?

Ejercicio A.2.35 Resolver los siguientes sistemas de ecuaciones:

$$\text{(I)}\begin{cases} x \equiv 2\,(\text{mód}\,3) \\ x \equiv 3\,(\text{mód}\,4) \end{cases} \qquad \text{(II)}\begin{cases} 2x \equiv 2\,(\text{mód}\,5) \\ 7x \equiv 4\,(\text{mód}\,10) \end{cases} \qquad \text{(III)}\begin{cases} x \equiv 1\,(\text{mód}\,2) \\ x \equiv 13\,(\text{mód}\,15) \\ x \equiv 7\,(\text{mód}\,17) \end{cases}$$

Ejercicio A.2.36 (Construcción de $\mathbb{R}$, mediante sucesiones de Cauchy). Para realizar este ejercicio es necesario conocer los resultados hasta la Sección II.4 incluida. Hemos visto como construir los números enteros $\mathbb{Z}$ a partir de los naturales $\mathbb{N}$ y podemos construir $\mathbb{Q}$ como el cuerpo de fracciones de $\mathbb{Z}$. El objetivo de este ejercicio es construir los números reales a partir del cuerpo de los números racionales $(\mathbb{Q},+,\cdot)$, mediante sucesiones de Cauchy (existen diversas construcciones equivalentes). Consideramos el conjunto de sucesiones de números racionales:

$$\mathbb{Q}^{\mathbb{N}} = \{(a_n)_{n=0}^{\infty} \ : \ a_n \in \mathbb{Q}, \forall n \in \mathbb{N}\}.$$

Sobre este conjunto definimos dos operaciones, la suma y el producto término a término:

$$\begin{aligned} (a_n)_{n=0}^{\infty} + (b_n)_{n=0}^{\infty} &:= (a_n + b_n)_{n=0}^{\infty}. \\ (a_n)_{n=0}^{\infty} \cdot (b_n)_{n=0}^{\infty} &:= (a_n \cdot b_n)_{n=0}^{\infty}. \end{aligned}$$

Se pide:

(I) Probar que $(\mathbb{Q}^{\mathbb{N}},+,\cdot)$ es un anillo conmutativo y unitario, pero no es un dominio de integridad.

(II) Recordamos que una sucesión $(a_n)_{n=0}^{\infty}$ se dice que es una **sucesión de Cauchy** si para todo $\varepsilon > 0$ existe $n_\varepsilon \in \mathbb{N}$ tal que para todos $n,m \in \mathbb{N}$ con $n,m \geq n_\varepsilon$ se tiene que $|a_n - a_m| < \varepsilon$. Consideramos el conjunto

$$A := \{(a_n)_{n=0}^{\infty} \in \mathbb{Q}^{\mathbb{N}} \ : \ (a_n)_{n=0}^{\infty} \text{ es de Cauchy}\}.$$

Probar que A es un subanillo de $\mathbb{Q}^{\mathbb{N}}$. ¿Es A un dominio de integridad?
(Pista: probar previamente que toda sucesión de Cauchy es acotada, es decir, que si $(a_n)_{n=0} \in A$, entonces existe $M > 0$ tal que $|a_n| \leq M$ para todo $n \in \mathbb{N}$).

(III) Consideramos el subconjunto:

$$I := \{(a_n)_{n=0}^{\infty} \in \mathbb{Q}^{\mathbb{N}} \ : \ \lim_{n\to\infty} a_n = 0 \ \}.$$

de $\mathbb{Q}^{\mathbb{N}}$. Probar que I es un ideal de A.

(IV) Probar que I es maximal en A y deducir que el anillo cociente $(A/I,+,\cdot)$ es un cuerpo. Llamamos **cuerpo de los números reales** a $\mathbb{R} = A/I$.

(V) Construir el inverso en $\mathbb{R} = A/I$ de la clase $[(x_n)_{n=0}^{\infty}] + I$ de la sucesión definida de forma recurrente por $x_1 = 2$ y $2x_{n+1} = x_n + (2/x_n)$ para todo $n \in \mathbb{N}$. ¿Qué número real representa $[(x_n)_{n=0}^{\infty}] + I$?

(VI) Construir un homomorfismo de anillos inyectivo de $\mathbb{Q}$ en $\mathbb{R} = A/I$ y deducir que $\mathbb{Q}$ es isomorfo a un subcuerpo de $\mathbb{R}$. *(Nota: podemos extender el orden de $\mathbb{Q}$ a $\mathbb{R}$ y construir este homomorfismo de forma que se preserve el orden.)*

A.3 El cuerpo de los números complejos

En esta sección se resumen las propiedades básicas para el manejo de los números complejos en la asignatura. El objetivo de este apéndice es repasar los contenidos que forman parte del currículo de Bachillerato y que el estudiante debe conocer. Los resultados y ejercicios presentados han sido extraídos fundamentalmente de [7, Capítulo 11] y se exponen con una estructura pareja.

Definición A.3.1 Un **número complejo** es un par ordenado de números reales. El conjunto de los número complejo se denota por $\mathbb{C}$, es decir, $\mathbb{C} = \{(a,b) : a,b \in \mathbb{R}\}$.

Si $z = (a,b)$ es un número complejo, a se denomina **parte real**, y se denota por $a = \mathrm{Re}\, z$, y b se denomina **parte imaginaria** de z, y se denota por $b = \mathrm{Im}\, z$.

Definimos en $\mathbb{C}$ las operaciones **suma** '$+$' y **producto** '$\cdot$' para todos $z = (a,b)$ y $w = (c,d)$ de $\mathbb{C}$ como sigue:

(A) $z + w = (a,b) + (c,d) := (a+c, b+d)$.

(B) $z \cdot w = (a,b) \cdot (c,d) := (a \cdot c - b \cdot d, ad + bc)$.

donde los signos de suma y producto en la expresión del lado derecho de las igualdades corresponden a las operaciones definidas en $\mathbb{R}$.

Notación A.3.2 Observamos que cada número complejo $z = (a,b)$ se puede escribir como

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

Denotamos por i al número complejo $(0,1)$, lo denominamos *unidad imaginaria*, y comprobamos que $i^2 = -1$. De este modo, el número (a,b) se representa por $a + bi$, representación que recibe el nombre de **expresión o forma binómica** del número $z = (a,b)$. Si identificamos un número real $a \in \mathbb{R}$ con el número complejo $(a,0)$ es lícito considerar $\mathbb{R}$ como subconjunto de $\mathbb{C}$. De esta manera, los números reales son aquéllos que tienen parte imaginaria nula.

Proposición A.3.3 $(\mathbb{C}, +, \cdot)$ es un **cuerpo**. En otras palabras, se verifica que:

(C.I) $(\mathbb{C}, +)$ es un **grupo conmutativo**. Equivalentemente, se cumple

- (C.I.A) la *propiedad asociativa:* para cualesquiera $z_1, z_2, z_3 \in \mathbb{C}$ se satisface que la igualdad $z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$.
- (C.I.B) la *existencia de elemento neutro:* existe un elemento que denotamos por 0 en $\mathbb{C}$ tal que para todo $z \in \mathbb{C}$ se tiene que $z + 0 = 0 + z = z$.
- (C.I.C) la *existencia de inverso:* para todo $z \in \mathbb{C}$ existe un elemento que denotamos por $-z$ en $\mathbb{C}$ tal que: $z + (-z) = (-z) + z = 0$.
- (C.I.D) la *propiedad conmutativa*: para todos $z_1, z_2 \in \mathbb{C}$ se tiene que $z_1 + z_2 = z_2 + z_1$.

(C.II) $(\mathbb{C}, \cdot)$ es un **monoide conmutativo** y $(\mathbb{C}\backslash\{0\}, \cdot)$ es un **grupo conmutativo**. Dicho de otro modo, el producto satisface las siguientes propiedades:

- (C.II.A) la *propiedad asociativa:* para cualesquiera $z_1, z_2, z_3 \in \mathbb{C}$ se satisface que la igualdad $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$.
- (C.II.B) la *existencia de elemento neutro:* existe un elemento que denotamos por 1 en $\mathbb{C}$ tal que para todo $z \in \mathbb{C}$ se tiene que $z \cdot 1 = 1 \cdot z = z$.
- (C.II.C) la *existencia de inverso en* $\mathbb{C}\backslash\{0\}$*:* para todo $z \in \mathbb{C}$, $z \neq 0$, existe un elemento que denotamos por z^{-1} en $\mathbb{C}$ tal que: $z \cdot z^{-1} = z^{-1} \cdot z = 1$.
- (C.II.D) la *propiedad conmutativa*: para todos $z_1, z_2 \in \mathbb{C}$ se tiene que $z_1 \cdot z_2 = z_2 \cdot z_1$.

(C.III) Se cumple la **propiedad distributiva** del producto respecto de la suma: para todos $z_1, z_2, z_3 \in \mathbb{C}$ se tiene que $z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$.

Definición A.3.4 Sea $z = a + bi$ un número complejo.
(A) El número complejo $a - bi = a + (-b)i$ se denomina **conjugado** de z y se denota por $\overline{z}$.
(B) El número real positivo $\sqrt{a^2 + b^2}$ se denomina **módulo** de z y se denota por $|z|$.

Ejemplos A.3.5 Empleando estas propiedades podemos realizar las propiedades elementales de la forma habitual:
(1) La suma: $(3+5i)+(-5+2i) = -2+7i$.
(2) La resta: $(3+5i)-(-5+2i) = 8-3i$.
(3) El producto: $(3+5i)(-5+2i) = -15+6i-25i+10i^2 = -15-10-19i = -25-19i$.
(4) El cociente:

$$\frac{3+5i}{-5+2i} \overset{\substack{\text{Multiplicando} \\ \text{por el conjugado}}}{=} \frac{3+5i}{-5+2i} \cdot \frac{-5-2i}{-5-2i} = \frac{-15-6i-25i+10}{25+4} = \frac{-5}{29} + \frac{-31}{29} i.$$

Propiedades A.3.6 — Propiedades del módulo y la conjugación. Sean z y w números complejos. Se verifica que:

(I) un número complejo z es real si y solo si $z = \overline{z}$.

(II) si z es real, el módulo de z coincide con el valor absoluto de z.

(III) $\overline{w+z} = \overline{w} + \overline{z}$ y $\overline{w \cdot z} = \overline{w} \cdot \overline{z}$. Si $w \neq 0$, entonces $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$.

(IV) $\mathrm{Re}\, z = \frac{z+\overline{z}}{2}$ e $\mathrm{Im}\, z = \frac{z-\overline{z}}{2i}$.

(V) $z \cdot \overline{z} = |z|^2$.

(VI) Si $z \neq 0$, entonces $z^{-1} = \frac{1}{z} = \frac{\overline{z}}{|z|^2}$.

(VII) $|z| = |\overline{z}|$.

(VIII) $|\mathrm{Re}\, z| \leq |z|$ y $|\mathrm{Im}\, z| \leq |z|$.

(IX) $|z \cdot w| = |z| \cdot |w|$. Si $w \neq 0$, entonces $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$.

(X) $|z+w| \leq |z| + |w|$.

(XI) $\big||z| - |w|\big| \leq |z-w|$.

Definición A.3.7 Si $z \in \mathbb{C}$, $z \neq 0$, un **argumento de** z es un número real θ tal que

$$\frac{z}{|z|} = \cos(\theta) + i\,\mathrm{sen}(\theta).$$

Si $\theta \in [-\pi, \pi)$ se dice que θ es el **argumento principal** de z. Si $z \in \mathbb{C}$, $z \neq 0$, se denota por $\mathrm{Arg}(z)$ al conjunto de todos los argumentos de z.

Observación A.3.8 El argumento de cero no está definido. Si $z \in \mathbb{C}$, $z \neq 0$, existen argumentos de z, es decir, $\mathrm{Arg}(z) \neq \emptyset$. Dado θ_0 un argumento de z, si $\theta_k = \theta_0 + 2\pi k$, con $k \in \mathbb{Z}$, se tiene que θ es un argumento de z y todos los argumento de z son de esa forma. En otras palabras, si $z \in \mathbb{C}$, $z \neq 0$ y θ_0 un argumento de z, entonces

$$\mathrm{Arg}(z) = \{\theta_0 + 2\pi k : k \in \mathbb{Z}\}.$$

Propiedades A.3.9 — Propiedades del argumento. Sean z y w números complejos con $z \neq 0$ y $w \neq 0$. Si α es un argumento de z y β es un argumento de w, entonces

(I) $\alpha + \beta$ es un argumento de $z \cdot w$.
(II) $-\alpha$ es un argumento de $\bar{z}$ y de $1/z$.
(III) $\alpha - \beta$ es un argumento de z/w.

Ejemplo A.3.10 (1) Si $x \in \mathbb{R}$, $x > 0$, entonces $\mathrm{Arg}(x) = \{2\pi k : k \in \mathbb{Z}\}$.
(2) Si $x \in \mathbb{R}$, $x > 0$, entonces $\mathrm{Arg}(x) = \{-\pi + 2\pi k : k \in \mathbb{Z}\}$.
(3) $\mathrm{Arg}(i) = \{\pi/2 + 2\pi k : k \in \mathbb{Z}\}$.
(4) $\mathrm{Arg}(1+i) = \{\pi/4 + 2\pi k : k \in \mathbb{Z}\}$.

Observación A.3.11 Si $z \in \mathbb{C}$, $z \neq 0$, y θ es un argumento de z, entonces

$$z = |z|(\cos(\theta) + i\,\mathrm{sen}(\theta)).$$

Esta representación que recibe el nombre de **expresión o forma trigonométrica** del número z. En estas condiciones se tiene que $\mathrm{Re}\, z = |z|\cos(\theta)$ e $\mathrm{Im}\, z = |z|\,\mathrm{sen}(\theta)$. Recíprocamente, si $z \in \mathbb{C}$, $z \neq 0$, y existe $\rho > 0$ tal que z se escribe como

$$z = \rho(\cos(\theta) + i\,\mathrm{sen}(\theta)),$$

entonces podemos probar que $\rho = |z|$ y que $\theta \in \mathrm{Arg}(z)$.

Proposición A.3.12 — Fórmula de Moivre. Si $n \in \mathbb{Z}$ y $z \in \mathbb{C}$, $z \neq 0$, y θ es un argumento de z, entonces

$$z^n = (|z|(\cos(\theta) + i\,\mathrm{sen}(\theta)))^n = |z|^n(\cos(n\theta) + i\,\mathrm{sen}(n\theta)).$$

Proposición A.3.13 — Raíz enésima de un número complejo. Sea $n \in \mathbb{N}_{\geq 1}$ y $z \in \mathbb{C}$, $z \neq 0$. Existen exactamente n números complejos distintos $w_0, w_1, \ldots w_{n-1}$ tales que para todo $k \in \{0, 1, 2, \ldots, n-1\}$ se tiene que $w_k^n = z$. Estos números reciben el nombre de **raíces enésismas de z**. Fijado un argumento θ_0 de z, se obtiene de la siguiente manera

$$w_k = |z|^{1/n}\left(\cos\left(\frac{\theta_0 + 2\pi k}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta_0 + 2\pi k}{n}\right)\right) \qquad \forall\, k \in \{0, 1, \ldots, n-1\}.$$

Definición A.3.14 Sea $z = x + iy \in \mathbb{C}$, con $x = \mathrm{Re}\, z$ e $y = \mathrm{Im}\, z$. Se define la **exponencial compleja** de z por

$$e^z = e^x(\cos(y) + i\,\mathrm{sen}(y)).$$

Observación A.3.15 Si $z \in \mathbb{C}$, $z \neq 0$, y θ es un argumento de z, entonces

$$z = |z|e^{i\theta}.$$

Esta representación que recibe el nombre de **expresión o forma polar** del número z. Con esta notación la Fórmula de Moivre se escribe como:

$$w_k = |z|^{1/n}\exp\left(i\left(\frac{\theta_0 + 2\pi k}{n}\right)\right) \qquad \forall\, k \in \{0, 1, \ldots, n-1\}.$$

donde w_k es una raíz enésismas de z y θ_0 es un argumento de z.

Ejemplos A.3.16 Multiplicaciones, divisiones, productos y raíces se calculan de un modo más sencillo en forma polar. Dados $a = 1+i$ y $b = 1+\sqrt{3}i$ obtenemos su forma polar $a = \sqrt{2}e^{i\pi/4}$ y $b = 2e^{i\pi/3}$.

(1) El producto: $a \cdot b = \sqrt{2}e^{i\pi/4}\,2e^{i\pi/3} = (2\sqrt{2})\,e^{i7\pi/12}$.

(2) El cociente:

$$\frac{a}{b} = \frac{\sqrt{2}e^{i\pi/4}}{2e^{i\pi/3}} = \frac{\sqrt{2}}{2}e^{-i\pi/12}.$$

(3) Potencias: $a^3 = (\sqrt{2}e^{i\pi/4})^3 = (2\sqrt{2})e^{i3\pi/4}$.

(4) Raíces: las raíces cúbicas de a son

$$w_0 = (2)^{1/6}e^{i\pi/12} \qquad w_1 = (2)^{1/6}e^{i9\pi/12} \qquad w_2 = (2)^{1/6}e^{i17\pi/12}.$$

Propiedades A.3.17 — Propiedades de la exponencial compleja. Se cumple que:

(I) Para números reales la exponencial compleja coincide con la exponencial real.

(II) si $z \in \mathbb{C}$ y $x = \operatorname{Re} z$, entonces $|e^z| = e^x$.

(III) si $z \in \mathbb{C}$ y $y = \operatorname{Im} z$, entonces y es un argumento de e^z.

(IV) si $z, w \in \mathbb{C}$, entonces $e^{z+w} = e^z e^w$.

(V) $e^z \neq 0$ para todo $z \in \mathbb{C}$.

(VI) si $z \in \mathbb{C}$, entonces $\overline{e^z} = e^{\bar{z}}$.

(VII) $e^z = 1$ si y solo si $z = 2\pi ki$ para algún $k \in \mathbb{Z}$.

(VIII) $e^{-z} = \dfrac{1}{e^z}$ para todo $z \in \mathbb{C}$.

(IX) $e^z = e^w$ si y solo si $z = w + 2\pi ki$ para algún $k \in \mathbb{Z}$.

Observación A.3.18 Aunque no se vamos a profundizar en esa cuestión, el estudiante debe notar que la definición del logaritmo complejo es más delicada que la del logaritmo en el caso real. Por ejemplo, teniendo presente la propiedad (VII), ¿cómo habría que definir el logaritmo de 1?

Ejercicio A.3.19 Probar las Propiedades A.3.6 .

Ejercicio A.3.20 Probar las Propiedades A.3.9.

Ejercicio A.3.21 Probar las Proposición A.3.12.

Ejercicio A.3.22 Probar las Propiedades A.3.17.

Ejercicio A.3.23 Determinar los números complejos $z \in \mathbb{C}$ que verifican $iz = \bar{z}$ y $|z - i| = 1$.

Ejercicio A.3.24 Sean z_1, z_2 números complejos. Demostrar que:

(I) $|z_1 + z_2|^2 = |z_1|^2 + |z_2|^2 + 2\operatorname{Re}(z_1\overline{z_2})$.

(II) $|1 - \overline{z_1}z_2|^2 - |z_1 - z_2|^2 = (1 - |z_1|^2)(1 - |z_2|^2)$.

(III) Si $|z_1| = 1$, entonces $|1 - \overline{z_1}z_2|^2 = |z_1 - z_2|$.

Ejercicio A.3.25 Sea $n \in \mathbb{N}_{\geq 1}$. Probar que si $z \in \mathbb{C}$ es solución de la ecuación $(z+1)^n + z^n = 0$, entonces $\operatorname{Re} z = -1/2$.

Ejercicio A.3.26 Sean $z, w \in \mathbb{C}$, $z \neq w$, tales que $r = \frac{(z+w)i}{z-w} \in \mathbb{R}$. Probar que $|z| = |w|$.

Ejercicio A.3.27 Determinar $z, w \in \mathbb{C}$ tales que $z + w = 3 + 2i$, $\operatorname{Re} z = 2$, $\operatorname{Re}(z/w) = 0$.

Ejercicio A.3.28 Dado $z = -1 + \sqrt{3}i$, hallar z^{-1}, z^{-3} y las raíces cuartas de z^{-1}.

Ejercicio A.3.29 Describir geométricamente los siguientes conjuntos:

(1) $A = \{z \in \mathbb{C} : |z - i| = 2\}$.
(2) $B = \{z \in \mathbb{C} : 1 < |z| < 4\}$.
(3) $C = \{z \in \mathbb{C} : \pi/3 \in \operatorname{Arg}(z)\}$.
(4) $D = \{z \in \mathbb{C} : -1 \leq \operatorname{Re}(z) \leq 3\}$.
(5) $E = \{z \in \mathbb{C} : -1 < \operatorname{Re}(z) < 3, 1 < \operatorname{Im}(z) < 5\}$.
(6) $F = \{z \in \mathbb{C} : \operatorname{Re}(z) < 0, \operatorname{Im}(z) > 0\}$.

Ejercicio A.3.30 Describir geométricamente los siguientes conjuntos:

$$A = \left\{ z \in \mathbb{C} : \operatorname{Re}\left(\frac{z-i}{z+i}\right) \right\}, \qquad B = \left\{ z \in \mathbb{C} : \operatorname{Im}\left(\frac{z-i}{z+i}\right) \right\}.$$

Ejercicio A.3.31 Sea $n \in \mathbb{N}_{\geq 2}$ y $\alpha \in \mathbb{C}$, $\alpha \neq 1$, tal que $\alpha^n = 1$. Demostrar que

$$\alpha + \alpha^2 + \cdots + \alpha^n = 0.$$

Ejercicio A.3.32 Opera y simplifica

(1) $\dfrac{(3-2i)(2+3i)}{3-4i}$ (2) $(1+i)^{2019}$ (3) $\dfrac{(\sqrt{3}-i)e^{i\frac{\pi}{12}}}{1-i}$.

Ejercicio A.3.33 Sean z y w números complejos no nulos tales que $(1+|z|^2)w = (1+|w|^2)z$. Probar que z y w tienen los mismos argumentos.

Ejercicio A.3.34 Calcular:
(1) Las raíces cuadradas de -4, $2i$, $1+i$ y $\sqrt{3}-i$.
(2) Las raíces cúbicas de 8, -1, $-i$ y $1-i$.
(3) Las raíces cuartas de $1+\sqrt{3}i$, $-9i$ y $(1+i)(1-i)^{-1}$.

Ejercicio A.3.35 Resolver las ecuaciones:
(1) $z^5 + 16z = 0$.
(2) $z^4 + 2z^2 + 1 = 0$.
(3) $z^{n-1} = \bar{z}$, con $n \in \mathbb{N}_{\geq 1}$ y $n > 2$.

Ejercicio A.3.36 Sean $\alpha = \sqrt{3} - i$ y $\beta = 1 - \sqrt{3}\,i$. Resolver las ecuaciones:
(1) $z^3 + \alpha z^2 + \beta z - i = 0$.
(2) $z^3 - (\beta/\overline{\alpha}) = 0$.
(3) $z^6 - 9z^3 + 8 = 0$.

Ejercicio A.3.37 Sea $n \in \mathbb{N}_{\geq 1}$. Demostrar la igualdad

$$\left(1 + e^{i\theta} + e^{i2\theta} + \cdots + e^{in\theta}\right) \operatorname{sen}\left(\frac{\theta}{2}\right) = \operatorname{sen}\left(\frac{(n+1)\theta}{2}\right) e^{in\theta/2}.$$

Ejercicio A.3.38 Sea $n \in \mathbb{N}_{\geq 2}$. Probar que el producto de todas las raíces enésimas de la unidad vale 1 o -1.

Bibliografía

Libros básicos

[8] Joseph A. Gallian. *Contemporary Abstract Algebra*. Brooks/Cole Cengage Learning, 2013. ISBN: 9781133599708 (véanse páginas 46, 50).

[9] Pierre Antoine Grillet. *Abstract Algebra*. Springer (2nd edition), 2007. ISBN: 978-0-387-71567-4 (véase página 116).

[12] Thomas W. Hungerford. *Algebra*. Springer (12th edition), 2003. ISBN: 9788497322072 (véase página 116).

Artículos

[1] Michael Brennan y Des Machale. "Variations on a Theme: A_4 Definitely Has No Subgroup of Order Six!" En: *Mathematics Magazine* (2000), páginas 36-40. DOI: 10.1080/0025570X.2000.11996796 (véase página 30).

[2] Chris K. Caldwell y Yeng Xiong. "What is the smallest prime?" En: *J. Integer Seq.* 15.9 (2012), Article 12.9.7, 14 (véase página 128).

[3] Chris K. Caldwell y col. "The history of the primality of one: a selection of sources". En: *J. Integer Seq.* 15.9 (2012), Article 12.9.8, 40 (véase página 128).

[4] Oscar A. Cámpoli. "A principal ideal domain that is not a Euclidean domain". En: *Amer. Math. Monthly* 95.9 (1988), páginas 868-871. ISSN: 0002-9890. DOI: 10.2307/2322908 (véase página 88).

[5] Pete L. Clark. "Factorization in Integral Domains". En: *(on-line) preprint, University of Georgia, Athens, GA.* (2010) (véase página 116).

[6] David J. Devries. "The group of units in Z_m". En: *Math. Mag.* 62.5 (1989), página 340. ISSN: 0025-570X. DOI: 10.2307/2689489 (véase página 116).

[10] David R. Guichard. “When Is U(n) Cyclic? An Algebraic Approach”. En: *Math. Mag.* 72.2 (1999), páginas 139-142. ISSN: 0025-570X (véase página 116).

[13] M. A. Jodeit Jr. “Uniqueness in the division algorithm”. En: *Amer. Math. Monthly* 74 (1967), páginas 835-836. ISSN: 0002-9890. DOI: 10.2307/2315810 (véase página 94).

[14] N. A. Khan. “Mathematical Notes: The Characteristic of a Ring”. En: *Amer. Math. Monthly* 70.7 (1963), página 736. ISSN: 0002-9890. DOI: 10.2307/2312257 (véase página 61).

[16] Lars–Daniel Öhman. “Are Induction and Well-Ordering Equivalent?” En: *The Mathematical Intelligencer* (2019), páginas 33-40. DOI: 10.1007/s00283-019-09898-4 (véase página 121).

Libros complementarios

[7] Félix Galindo Soto, Javier Sanz Gil y Luis A. Tristán Vega. *Guía práctica de cálculo infinitesimal en una variable real*. Ediciones Paraninfo, S.A, 2003. ISBN: 9788497322072 (véase página 134).

[11] John F. Humphreys. *A Course in Group Theory*. Oxford University Press, 1996. ISBN: 9780198534532 (véase página 116).

[15] Lang. *Algebra*. Springer, 2002. ISBN: 978-0-387-71567-4 (véase página 116).

[17] Giuseppe Peano. *Arithmetices principia: nova methodo*. Torino, Fratres Bocca, 1889 (véase página 119).

[18] Giuseppe Peano. *Formulario mathematico*. 5.ª edición. Torino, Fratres Bocca, 1908 (véase página 119).

Índice alfabético

p-grupo, 49

anillo, 53
anillo cociente, 59
anillo conmutativo, 53
anillo de polinomios, 94
anillo Noetheriano, 85
anillo unitario, 53
automorfismo, 37

característica de un anillo, 61
característica de un anillo unitario, 61
centralizador de un elemento, 49
centro de un grupo, 11
ciclo, 19
clase de conjugación, 49
clases laterales, 26
congruencias, 129
construcción de $\mathbb{C}$, 133
construcción de $\mathbb{Q}$, 129
construcción de $\mathbb{R}$, 132
construcción de $\mathbb{Z}$, 121
Criterio de Eisenstein, 113
Criterio de irreducibilidad módulo p , 112
Criterio de traslación, 114
cuaterniones de Hamilton, 11
cuerpo de fracciones, 76

divisor, 54
divisor de cero, 54
dominio de factorización única (D.F.U.), 81
dominio de ideales principales (D.I.P.), 84
dominio euclídeo (D.E.), 87
dominio, dominio de integridad, 70

ecuaciones diofánticas, 130
elemento inverso/opuesto, 5
elemento irreducible, 79
elemento neutro, 5
elemento primo, 79
elementos asociados, 78
endomorfismo, 37
Enteros de Gauss, 56
enteros módulo n, 7
evaluación de un polinomio, 99

función de Euler, 130

grado de un polinomio, 96
grupo, 5
grupo cociente, 33
grupo cíclico, 12
grupo de permutaciones, 18
grupo diédrico, 7
grupo producto, 8
grupo simétrico, 18
grupos isomorfos, 37

homomorfismo de anillos, 63
homomorfismo de grupos, 37

ideal, 57

ideal generado por un subconjunto, 58
ideal maximal, 73
ideal primo, 73
ideal principal, 84
ideal suma, 59
idempotente, 55
Identidad de Bezout en $\mathbb{Z}$, 124
imagen de un homomorfismo, 38
isomorfismo, 37
isomorfismo de anillos, 64

monoide, 5
multiplicidad de una raíz, 104
máximo común divisor, 82
mínimo común múltiplo, 83
múltiplo, 54

nilpotente, 55
notación aditiva/multiplicativa, 6
núcleo de un homomorfismo, 38

orden de un elemento, 13
orden de un grupo, 13

Pequeño Teorema de Fermat, 131
permutaciones disjuntas, 19
permutación, 18
permutación par/impar, 24
polinomio primitivo, 107
Primer Teorema de Isomorfía, 41, 64
propiedad asociativa, 5
propiedad conmutativa, 5

raíz o cero de un polinomio, 99
relaciones módulo S, 26

Segundo Teorema de Isomorfía, 42, 65
semigrupo, 5
sistema completo de representantes, 30
subgrupo, 8
subgrupo generado por un subconjunto, 10
subgrupo normal, 31

Teorema chino del resto, 66
Teorema chino del resto en $\mathbb{Z}$, 131
Teorema de Cauchy (grupos abelianos), 34
Teorema de Cauchy (grupos no abelianos), 50
Teorema de Euler, 131
Teorema de la raíz racional, 112
Teorema de Lagrange, 29
Teorema fundamental de grupos abelianos finitos , 48
Tercer Teorema de Isomorfía, 42, 66
Test de caracterización de ideales , 57
Test de caracterización de subanillos, 55
Test de caracterización de subgrupos, 8
transposición, 19

unidad, 54

índice de un subgrupo, 29