Apuntes de Estructuras Algebraicas

Francisco Javier Gallego Rodrigo

23 de julio de 2026

Índice

Introducción **5**

1 Generalidades sobre anillos **11**
1.1 Primeras propiedades y ejemplos 11
1.2 Divisores de cero. Unidades 18
1.3 Subanillos 20
1.4 Cuerpo de fracciones 22

2 Ideales. Homomorfismos de anillos **26**
2.1 Ideales 26
2.2 Anillo cociente 32
2.3 Homomorfismos de anillos 35
2.4 El teorema de isomorfía 44
2.5 Ideales primos e ideales maximales 50
2.6 Teorema chino del resto 55

3 Divisibilidad **60**
3.1 Dominios euclídeos 60
3.2 Dominios de ideales principales 64
3.3 Dominios de factorización única 70
3.4 Máximo común divisor 76
3.5 Sistemas de congruencias 82

4 Factorialidad en anillos de polinomios **85**
4.1 Raíces de un polinomio 85
4.2 El criterio modular 87
4.3 Irreducibilidad en $R[X]$ frente a irreducibilidad en $K[X]$ 89
4.4 Si R es un dominio de factorización única, entonces $R[X]$ es un dominio de factorización única 93
4.5 El criterio de Eisenstein 94

5 Generalidades sobre grupos **97**
5.1 Primeras propiedades y ejemplos 97

5.2 Subgrupos 99
5.3 El grupo diédrico 101
5.4 Grupos cíclicos 104
5.5 Índice de un subgrupo 109

6 Homomorfismos de grupos. Subgrupos normales 114
6.1 Homomorfismos de grupos 114
6.2 Subgrupos normales 120
6.3 Grupo cociente 124

7 El grupo simétrico 127
7.1 Primeras definiciones 127
7.2 Descomposición de una permutación 130
7.3 El grupo alternado 133

8 Acción de un grupo en un conjunto 137
8.1 Definiciones y ejemplos 137
8.2 Órbitas de una acción 144
8.3 Orden del estabilizador y cardinal de la órbita 148

9 Estructura de los grupos abelianos finitamente generados 151
9.1 Generadores y relaciones 151
9.2 El teorema de estructura 155

Apéndice: Clases y conjunto cociente de una relación de equivalencia

Introducción

Una de las características del Álgebra es el uso de la abstración. A veces nos damos cuenta de que varias situaciones concretas, varios problemas concretos responden a un mismo patrón. Comprender las propiedades de ese patrón, propiedades que por serlo del patrón común son comunes a todos los problemas que encajan en ese patrón, nos puede servir para resolver todos esos problemas a la vez, usando un único argumento. Pondremos un ejemplo que viene del Álgebra Lineal: "Todas las matrices cuadradas con coeficientes reales y determinante no nulo son invertibles". Este hecho lo habrás visto demostrado para una matriz general de orden n, una matriz "abstracta" (no para una concreta, con coeficientes concretos). ¿Cuál fue la ventaja de hacerlo así? Que cuando te daban cualquier matriz concreta con determinante no nulo, sabías que era invertible, sin necesidad de comprobar o demostrar este hecho cada vez. Aunque existen infinitas matrices con el determinante no nulo, una sola demostración basta para probar que todas tienen inversa. En otros casos, aumentar el grado de abstración también es útil al enfrentarnos a un problema concreto, ya que es posible que tengamos demasiados datos particulares que no nos ayuden a resolverlo sino, más bien, nos distraigan. En cambio, lo que quizá sí nos ayude es ese patrón más general. Como dice el dicho, a veces el árbol no nos deja ver el bosque y necesitamos elevarnos hasta un nivel de abstración superior para ver el bosque, su forma, los caminos que lo recorren...

Así pues, este será de alguna forma el *leitmotiv* de este curso: encontrar qué tienen en común varios objetos, en apariencia distintos. Por ejemplo, ¿qué piensas que tienen en común el conjunto de los números enteros $\mathbf{Z}$, el conjunto de los polinomios en una variable con coeficientes reales $\mathbf{R}[X]$ o el conjunto las funciones continuas de $\mathbf{R}$ en $\mathbf{R}$? Lo que tienen en común es que son ejemplos de la misma *estructura algebraica*, pues son los tres ejemplos de *anillos conmutativos unitarios*. Al igual que en el caso de las matrices con determinante no nulo, vamos a demostrar muchas propiedades de los anillos conmutativos unitarios. Lo haremos estudiándolos en general, es decir, de manera abstracta. Por eso este estudio no lo tendremos que hacer tres veces, una para $\mathbf{Z}$, otra para $\mathbf{R}[X]$ y otra más para el conjunto de las funciones continuas de $\mathbf{R}$ en $\mathbf{R}$ sino que bastará hacer este estudio una sola vez. Además, las propiedades que vayamos descubriendo para los anillos conmutativos unitarios se aplicarán no solo a estos tres que hemos mencionado sino a cualquier otro ejemplo de anillo conmutativo unitario que nos encontremos (o, ciertamente, para cualquier otro ejemplo de anillo conmutativo

unitario, conozcamos nosotros su existencia o no).

Esta es la filosofía del Álgebra Abstracta y es una filosofía muy potente. Tiene la desventaja de que, a veces, es difícil acostumbrarnos a este nivel de abstración (muchas personas están más cómodas pensando en situaciones y ejemplos concretos). Así pues, en este curso trataremos de mantener un equilibrio entre ese nivel más abstracto y el nivel más concreto de los ejemplos, intentando que los ejemplos ilustren y motiven los conceptos e ideas más abstractos propios del Álgebra (así, si un concepto te resulta muy abstracto, puede ayudarte pensarlo en un ejemplo concreto adecuado). Intentaremos además que los primeros ejemplos motivadores que veamos sean ejemplos que resulten familiares (como $\mathbf{Z}$, que conoces desde la ESO, o los polinomios en una variable y coeficientes reales).[1]

Volvamos al concepto de estructura algebraica que da nombre al curso. Hay una estructura algebraica que has estudiado con detenimiento en la asignatura de Álgebra Lineal, la estructura de espacio vectorial. En la asignatura presente nos vamos a centrar en el estudio de otras dos estructuras, la estructura de anillo (conmutativo unitario) y la estructura de *grupo*. Antes de pasar a definirlas, vamos a jugar un poco con ejemplos concretos. El objetivo es convencerte de que, los anillos y los grupos son objetos que ya conoces o, al menos, son estructuras algebraicas de las que ya conoces ejemplos. Y, ¿qué es eso de una estructura algebraica? Recordemos otra vez el caso de los espacios vectoriales. Un ejemplo de espacio vectorial es $\mathbf{R}^2$, que es el conjunto de pares ordenados de números reales. Pero, ¿un espacio vectorial es simplemente un conjunto, o hay que añadir algo más para dotarle de estructura? En otras palabras, ¿qué nos hace falta considerar en el conjunto $\mathbf{R}^2$ para dotarle de estructura de espacio vectorial? Nos hace falta considerar una *operación interna* (la suma) y una *operación externa* (el producto por escalares). Así pues, $\mathbf{R}^2$ equipado con esas dos operaciones (que cumplen una serie de propiedades, ocho concretamente) es un espacio vectorial. Los anillos y los grupos también son conjuntos equipados de operaciones, internas en este caso, que satisfacen ciertas propiedades.

Cuando estas operaciones son dos, la estructura que tenemos es un anillo. Si pensamos en un conjunto equipado con dos operaciones internas, seguramente el primer ejemplo que nos viene a la cabeza es $\mathbf{Z}$, el conjunto de números enteros, en el que tenemos definidas la suma y el producto. La suma de números enteros cumple las propiedades *asociativa*, *conmutativa*, existencia de *elemento neutro* y existencia de *elemento opuesto*. El

[1] De hecho, este camino entre lo concreto y lo abstracto que nosotros vamos a recorrer en un cuatrimestre, historicamente duró varias décadas. Este proceso histórico no fue *deductivo* sino *inductivo*, ya que primero se estudiaron los casos particulares y, bastante después, se desarrollaron los conceptos abstractos generales. Así, durante muchos años los matemáticos estuvieron trabajando con diversos ejemplos de *grupos* (al menos desde los trabajos de E. Galois de la principios del siglo XIX) y de anillos (desde R. Dedekind, en la década de 1870) antes de que se formularan las definiciones abstractas de grupo (W. von Dyck en 1882) y de anillo (A. Fraenkel en 1914 y E. Noether en 1921). Nosotros no reproduciremos este proceso desde los ejemplos concretos hasta las definiciones abstractas sino que, aunque motivadas por ejemplos, dispondremos desde el principio de esas definiciones. Esto nos permitirá deducir propiedades válidas para todos los ejemplos concretos que tratemos.

producto de números enteros cumple las propiedades asociativa, conmutativa y existencia de elemento neutro. La suma y el producto cumplen la propiedad *distributiva*. Pues bien, todo conjunto no vacío con dos operaciones internas que cumplan las mismas propiedades que hemos enumerado para la suma y el producto de números enteros es un anillo conmutativo unitario y comparte con $\mathbf{Z}$ muchas otras propiedades. Otro ejemplo de conjunto con dos operaciones que cumplen las mismas propiedades que hemos mencionado para la suma y el producto en $\mathbf{Z}$ es $\mathbf{Q}$, el conjunto formado por los números racionales equipado con la suma y el producto que conoces. En este caso el producto cumple una propiedad adicional: cada elemento no nulo tiene *inverso*. Por ello $\mathbf{Q}$ pertenece a un tipo especial de anillo conmutativo unitario que llamamos *cuerpo*. Otro ejemplo de conjunto equipado con dos operaciones internas es el de las matrices $n \times m$ con elementos reales, con la suma y el producto de matrices. En este caso, el producto no cumple la propiedad conmutativa, por lo que las matrices $n \times m$ con elementos reales son un anillo unitario no conmutativo. En general, un anillo es un conjunto no vacío con dos operaciones internas que cumplen las mismas propiedades enumeradas para la suma y el producto en $\mathbf{Z}$, excepto quizá la conmutativa y/o el elemento neutro del producto. Como has visto, aunque no te hayas encontrado nunca hasta ahora en Matemáticas con la palabra anillo, hay varios ejemplos de anillos que te son muy familiares.

Si en un conjunto solo estamos considerando una operación interna y esta cumple las propiedades asociativa, existencia de neutro y existencia de inverso, estamos ante la estructura de *grupo*. Un ejemplo de grupo es el formando por el conjunto $\mathbf{Q}^*$ de los números racionales no nulos; la operación interna que consideramos en este caso es el producto. En este caso, además de las propiedades mencionadas, el producto cumple la propiedad conmutativa, por lo que $\mathbf{Q}^*$ es un grupo *conmutativo* o *abeliano*. Otro ejemplo de grupo, esta vez no conmutativo, es el de las matrices cuadradas de orden 2 y determinante no nulo, con el producto de matrices. Igual que antes, aunque no hayas visto antes la noción de grupo hay varios ejemplos de grupos que ya conoces.

Las estructuras que vamos a estudiar en este curso son los grupos y los anillos. Los cuerpos también aparecerán, pero son un caso particular de anillo. Parecería que los grupos, al tener una sola operación interna, son más sencillos de estudiar que los anillos, pero no es así. Para empezar, no estudiaremos anillos en toda su generalidad sino que nos centraremos en los anillos conmutativos unitarios. Los anillos no conmutativos y/o sin unidad son más complicados y no profundizaremos en ellos en este curso. En cambio sí trataremos grupos abelianos y no abelianos. Estos últimos presentan la dificultad de que su operación interna no es conmutativa. Además, ya vimos que el ejemplo más sencillo de anillo conmutativo unitario, $\mathbf{Z}$ con la suma y el producto usuales, nos es muy conocido. Este ejemplo tan natural es un buen punto de partida para comenzar a partir de él la abstracción de la que hemos hablado. Por ello empezaremos introduciendo el concepto de anillo para pasar enseguida a estudiar los anillos conmutativos unitarios.

A continuación damos las definiciones formales que las nociones que hemos avanzado en los párrafos anteriores:

Definición 0.1.1. Un grupo $(G, *)$ es un conjunto no vacío G junto con una operación interna

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

que satisface las siguientes propiedades:

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

(2) Elemento neutro: existe $1 \in G$ tal que $a * 1 = 1 * a = a$ para todo $a \in G$.

(3) Elemento inverso: para cada elemento $a \in G$ existe un elemento $a' \in G$ que verifica $a * a' = a' * a = 1$.

Si además se cumple la propiedad:

(4) Conmutativa: $a * b = b * a$ para cualesquiera $a, b \in G$

decimos que el grupo es conmutativo o abeliano.

Definición 0.1.2. Un anillo $(R, +, \cdot)$ es un conjunto no vacío R, junto con dos operaciones internas, que llamaremos suma y producto,

$$\begin{array}{rccc} + : & R \times R & \longrightarrow & R \\ & (r, s) & \mapsto & r + s \end{array}$$

$$\begin{array}{rccc} \cdot : & R \times R & \longrightarrow & R \\ & (r, s) & \mapsto & r \cdot s \end{array}$$

que satisfacen las siguientes propiedades:

(1) Asociativa de la suma: $(r + s) + t = r + (s + t)$ para cualesquiera $r, s, t \in R$.

(2) Conmutativa de la suma: $r + s = s + r$ para cualesquiera $r, s \in R$.

(3) Elemento neutro de la suma: Existe $0 \in R$ tal que $r + 0 = r$ para todo $r \in R$.

(4) Elemento opuesto: para todo $r \in R$ existe $r' \in R$ tal que $r + r' = 0$.

(5) Asociativa del producto: $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ para todos $r, s, t \in R$.

(6) Distributiva del producto respecto de la suma.

$$r \cdot (s + t) = r \cdot s + r \cdot t,$$
$$(r + s) \cdot t = r \cdot t + s \cdot t,$$

para cualesquiera $r, s, t \in R$.

Si además de las propiedades de (1) a (6) se cumple la propiedad

(7) Conmutativa del producto: $r \cdot s = s \cdot r$ para cualesquiera $r, s \in R$

decimos que el anillo es *conmutativo*.

Si además de las propiedades de (1) a (6) se cumple la propiedad

(8) Elemento neutro del producto: existe $1 \in R$ tal que $1 \cdot r = r \cdot 1 = r$ para todo $r \in R$

decimos que el anillo es *unitario* o con *elemento unidad*.

Observación 0.1.3. Si R es un anillo, entonces $(R, +)$ es un grupo abeliano.

Definición 0.1.4. Sea $\mathbf{k}$ un anillo conmutativo unitario. Si $\mathbf{k} \neq 0$ y para todo $r \in \mathbf{k}, r \neq 0$, existe $\tilde{r} \in R$ tal que $r \cdot \tilde{r} = 1$, decimos que $\mathbf{k}$ es un cuerpo.

PARTE I: ANILLOS

Tema 1

Generalidades sobre anillos

1.1 Primeras propiedades y ejemplos

Notación 1.1.1. Sea R un anillo y sean $r, s \in R$. En ocasiones omitiremos el símbolo $\cdot$ escribiendo rs en lugar de $r \cdot s$.

Ejemplo 1.1.2. El conjunto de los números enteros $\mathbf{Z}$ con la suma y el producto usuales es un anillo conmutativo unitario.

Ejemplo 1.1.3. Sea $n \in \mathbf{N}, n > 1$. El conjunto formado por los números enteros múltiplos de n con la suma y el producto usuales es un anillo conmutativo no unitario.

Ejemplo 1.1.4. El conjunto $\mathbf{Q}$ de los números racionales, el conjunto $\mathbf{R}$ de los números reales y el conjunto $\mathbf{C}$ de los números complejos, con la suma y producto usuales, son cuerpos.

Ejemplo 1.1.5. En la definición (propiedad (8) de la definición 0.1.2) de anillo unitario no exigimos $1 \neq 0$. Si en un anillo unitario R se da $0 = 1$, entonces R tiene un solo elemento, ya que para todo $r \in R$ se tiene $r = 1r = 0r = 0$, por lo que $R = \{0\}$, es decir, R es el anillo *nulo* o anillo *trivial*.

Antes de introducir más ejemplos, vemos las siguientes propiedades, que son consecuencias inmediatas de la definición 0.1.2:

Observación 1.1.6. Sea R un anillo y sean $r, s \in R$.

(1) El elemento neutro de la suma es único. En efecto, si 0 y $0'$ verifican ambos la propiedad (3) de la definición 0.1.2, entonces, por las propiedades (2) y (3) de la definición 0.1.2, $0 = 0 + 0' = 0' + 0 = 0'$.

(2) Para cada $r \in R$ su elemento opuesto es único. En efecto, si existen r' y r'' tales que $r + r' = r + r'' = 0$, por (1), (2), (3) y (4) de la definición 0.1.2 tenemos $r' = r' + 0 = r' + (r + r'') = (r' + r) + r'' = 0 + r'' = -r''$.

Denotaremos al opuesto de r como $-r$ y escribiremos $r + (-s) = r - s$.

(3) $-(-r) = r$, es decir, el opuesto de $-r$ es r.

(4) Para todo $r \in R$, se tiene $0r = r0 = 0$. En efecto, $0r = (0+0)r = 0r + 0r$. Si llamamos $s = 0r$, tenemos $s = s + s$ y $0 = s - s = (s+s) - s = s + (s - s) = s + 0 = s$. La igualdad $r0 = 0$ se demuestra de manera análoga.

(5) $(-r)s = r(-s) = -(rs)$. En efecto, por la propiedad (6) de la definición 0.1.2 y por (4), $rs + (-r)s = (r - r)s = 0s = 0$. Que $r(-s) = -(rs)$ se demuestra de la misma manera.

(6) $(-r)(-s) = rs$. En efecto, de (3) y (5) se sigue $(-r)(-s) = -(r(-s)) = -(-(rs)) = rs$.

Sea ahora R un anillo unitario.

(7) El elemento neutro del producto es único. En efecto, si 1 y 1′ verifican ambos la propiedad (8) de la definición 0.1.2, entonces, por dicha propiedad, $1 = 1 \cdot 1' = 1'$.

(8) $-r = (-1)r$. En efecto, por la propiedad (8) de la definición 0.1.2 y (5), tenemos $(-1)r = -(1r) = r$.

Notación 1.1.7. (1) Como la suma cumple la propiedad asociativa (propiedad (1) de la definición 0.1.2), no es ambiguo escribir $r + s + t$, que quiere decir $(r + s) + t$ (o $r + (s + t)$). Procederemos de igual forma para sumas de más de tres términos.

(2) De igual forma, como el producto cumple la propiedad asociativa (propiedad (5) de la definición 0.1.2), no es ambiguo escribir rst, que querrá decir $(rs)t$ (o $r(st)$). Procederemos de igual forma para productos de más de tres términos.

(3) Si $n \in \mathbf{N}$, nr significará $r + \overset{n)}{\cdots} + r$ y $(-n)r$ significará $-r - \overset{n)}{\cdots} - r$ (de hecho, $(-n)r = -(nr)$). ¡Cuidado! En este apartado el signo $-$ sirve unas veces para denotar el opuesto de un elemento $\mathbf{Z}$ y, otras veces, el opuesto de un elemento en R.

(4) Si $n \in \mathbf{N}$, r^n significará $r \overset{n)}{\cdots} r$; para $0 \in \mathbf{Z}$, r^0 significará 1.

Observación 1.1.8. Sea R un anillo y sean $r, s \in R$. Si $rs = sr$, entonces

$$(r+s)^n = \sum_{k=0}^{n} \binom{n}{k} r^{n-k} s^k. \tag{1.1.8.1}$$

Por tanto, si R es conmutativo, la fórmula (1.1.8.1) se cumple para cualesquiera $r, s \in R$, pero si R no es conmutativo (por ejemplo, si $R = M_n(\mathbf{k}), n > 1$), existen $r, s \in R$ para los que la fórmula (1.1.8.1) no se cumple.

Ejemplo 1.1.9. (1) Sea $\mathbf{k}$ un cuerpo (por ejemplo, $\mathbf{Q}, \mathbf{R}$ o $\mathbf{C}$). Un polinomio en una variable con coeficientes en $\mathbf{k}$ es una expresión de la forma $a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$, donde $m \in \mathbf{N} \cup \{0\}$, $a_0, a_1, a_2, \ldots, a_m \in \mathbf{k}$ y X es la variable. En el conjunto de todos

estos polinomios, que denotaremos por $\mathbf{k}[X]$, definimos la suma y el producto usuales: si

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m \text{ y } g(X) = b_0 + b_1X + b_2X^2 + \cdots + b_lX^l$$

entonces el término k–ésimo del polinomio $f + g$ es

$$(a_k + b_k)X^k \tag{1.1.9.1}$$

definiendo $a_k = 0$ si $k > n$ y $b_k = 0$ si $k > l$; por otra parte, el término k–ésimo del polinomio $f \cdot g$ es

$$(a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \cdots + a_{k-1}b_1 + a_kb_0)X^k. \tag{1.1.9.2}$$

Con esta suma y este producto $\mathbf{k}[X]$ es un anillo conmutativo unitario.

(2) Más en general, sea R un anillo. Podemos definir el conjunto $R[X]$ de los polinomios en una variable con coeficientes en R. Este conjunto es un anillo (conmutativo o unitario si y solo si R es conmutativo o unitario) con respecto a la suma y el producto definidos de manera análoga a la suma y el producto de $\mathbf{k}[X]$.

Definición 1.1.10. Sea R un anillo. Sea $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$ un polinomio no nulo de $R[X]$ tal que $a_m \neq 0$. El *grado* (en X) de $f(X)$ es $\text{gr}(f) = m$. Si $f(X)$ es el polinomio constante nulo, el grado (en X) de $f(X)$ es $\text{gr}(f) = -\infty$.

Ejemplo 1.1.11. Acabamos de ver que, a partir de un anillo R, podemos construir un nuevo anillo $R[X]$. Partiendo ahora de ese nuevo anillo $R[X]$ podemos construir otro anillo más, el anillo de polinomios en una variable, llamémosla Y para evitar confusiones, con coeficientes en el anillo $R[X]$. Es decir, tendríamos el anillo $R[X][Y]$, cuyos elementos, como veremos en la observación 1.1.12, podemos entender como polinomios en dos variables (X e Y) y coeficientes en R. Este proceso se puede extender de manera inductiva a cualquier número finito de variables. Así, definimos $R[X_1, \ldots, X_n]$ inductivamente de la siguiente manera: $R[X_1, \ldots, X_n] := R[X_1, \ldots, X_{n-1}][X_n]$.

Observación 1.1.12. Usando la definición de suma término a término no es difícil ver que los polinomios de $R[X_1, \ldots, X_n]$ se escriben como suma finita de monomios en las variables $X_1, \ldots, X_n$, multiplicados cada uno por un coeficiente en R. Vemos cómo lo haríamos para un polinomio concreto, por ejemplo de $\mathbf{Z}[X, Y]$. Recordemos que hemos definido $\mathbf{Z}[X, Y]$ como $\mathbf{Z}[X][Y]$, por lo que los elementos de $\mathbf{Z}[X, Y]$ son de la forma $a_0 + a_1Y + a_2Y^2 + \cdots + a_nY^n$, con $n \in \mathbf{N} \cup \{0\}$ y $a_0, a_1, a_2, \ldots, a_n \in \mathbf{Z}[X]$, es decir, son polinomios en una variable X con coeficientes en $\mathbf{Z}$. Así, un elemento de $\mathbf{Z}[X][Y]$ sería por ejemplo

$$f = (2 + X - X^2) + (3X + 5X^3 + X^4)Y + (1 - 2X^2)Y^3.$$

Denotemos $S = \mathbf{Z}[X]$. Por la definición de suma (1.1.9.1) en $S[Y]$, el término $(3X + 5X^3 + X^4)Y$ de f es la suma de tres polinomios de $S[Y]$, a saber, $(3X)Y$, $(5X^3)Y$ y $(X^4)Y$. Si nos

fijamos por ejemplo en $(5X^3)Y$ vemos que 5, X^3 e Y son tres polinomios de $S[Y]$ (los dos primeros de grado 0 y el último de grado 1). Por la propiedad asociativa del producto en $S[Y]$, $(5X^3)Y = 5(X^3Y)$ y, según la notación 1.1.7 (2), $(5X^3)Y$ se puede escribir $5X^3Y$. De igual forma, $(3X)Y = 3XY$ y $(X^4)Y = X^4Y$. Razonando igual para los otros términos $2 + X - X^2$ y $(1 - 2X^2)Y^3$ de f y por las propiedades asociativa y conmutativa de la suma y la notación 1.1.7 (1), podemos escribir f como

$$f = 2 + X - X^2 + 3XY + Y^3 + 5X^3Y + X^4Y - 2X^2Y^3, \tag{1.1.12.1}$$

(hemos usado la propiedad conmutativa de la suma para ordenar los sumandos de (1.1.12.1) según el *grado total* de cada monomio (véase la definición 1.1.14 (1)))

Observación 1.1.13. Como se mencionó en el ejemplo 1.1.9, $R[X_1, \ldots, X_n]$ no tiene por qué ser conmutativo (lo es si y solo si el anillo R lo es). Aun así, las variables $X_1, \ldots, X_n$ sí "conmutan". Lo vemos para dos variables. Llamamos $S = R[X]$. Entonces, según el ejemplo 1.1.11, $R[X, Y]$ es $S[Y]$. Sean $a, b \in R, a, b \neq 0$. Entonces aX y bY son dos polinomios de $S[Y]$, el primero de grado 0 (en Y) y el segundo de grado 1 (en Y). Entonces $(aX)(bY)$ es, según la definición (1.1.9.2) del producto en $S[Y]$ y en $R[X]$

$$(aX)(bY) = ((aX)b)Y = ((ab)X)Y.$$

Por otra parte $(aY)(bX)$ es, según la definición (1.1.9.2) del producto en $S[Y]$ y en $R[X]$

$$(aY)(bX) = (a(bX))Y = ((ab)X)Y.$$

Por tanto $(aX)(bY) = (aY)(bX)$. Si R es un anillo unitario, el mismo argumento nos dice que $XY = YX$.

Definición 1.1.14. Sea R un anillo.

(1) Sea $a \in R, a \neq 0$ y sea $aX_1^{m_1}X_2^{m_2}\cdots X_n^{m_n}$ un monomio de $R[X_1, \ldots, X_n]$. El *grado total* (en $X_1, X_2, \ldots, X_n$) de $aX_1^{m_1}X_2^{m_2}\cdots X_n^{m_n}$ es $m_1 + m_2 + \cdots + m_n$.

(2) Sea $f(X_1, \ldots, X_n)$ un polinomio no nulo de $R[X_1, \ldots, X_n]$. El *grado total* (en $X_1, X_2, \ldots, X_n$) de $f(X_1, \ldots, X_n)$ es el máximo de los grados totales de los monomios de $f(X_1, \ldots, X_n)$. Si $f(X_1, \ldots, X_n)$ es el polinomio constante nulo, el grado total (en X) de $f(X)$ es $-\infty$.

Ejemplo 1.1.15. El conjunto $\mathscr{C}(\mathbf{R}, \mathbf{R})$ de las funciones continuas de $\mathbf{R}$ en $\mathbf{R}$ es un anillo con respecto a la suma y el producto de funciones. En efecto, como la suma y el producto de funciones continuas son funciones continuas, la suma y el producto son operaciones internas en $\mathscr{C}(\mathbf{R}, \mathbf{R})$. Comprobamos algunas de las 8 propiedades de la definición 0.1.2. Las propiedades (1), (2), (5), (6) y (7) se siguen del hecho de que $\mathbf{R}$ cumple también esas propiedades al ser $\mathbf{R}$ un anillo. Las funciones constantes 0 y 1 son funciones continuas y son respectivamente los elementos neutros de la suma y del producto. Finalmente, si f es una función continua, la función $-f$ definida como $(-f)(x) = -(f(x))$ también lo es y es el elemento opuesto de f.

El ejemplo 1.1.15 se puede generalizar como sigue.

Ejemplo 1.1.16. Sea X un conjunto no vacío y sea R un anillo. El conjunto de aplicaciones $\mathscr{A}(X,R)$ de X a R es un anillo con la suma y el producto definidos así: si $f_1, f_2 \in \mathscr{A}(X,R)$, entonces $(f_1+f_2)(x) = f_1(x)+f_2(x)$ y $(f_1 \cdot f_2)(x) = f_1(x)\cdot f_2(x)$ para todo x, donde $f_1(x)+f_2(x)$ y $f_1(x)\cdot f_2(x)$ es la suma y el producto de $f_1(x)$ y $f_2(x)$ como elementos de R. Imitando los argumentos del ejemplo 1.1.15 es fácil demostrar que $\mathscr{A}(X,R)$ es un anillo (conmutativo y/o unitario si y solo si R es conmutativo y/o unitario) respecto a esas operaciones.

Ejemplo 1.1.17. Una función $f : \mathbf{R} \to \mathbf{R}$ se dice de soporte compacto si existen $a \leq b \in \mathbf{R}$ tales que $f(x) = 0$ si $x \notin [a,b]$. El conjunto de las funciones de soporte compacto con la suma y el producto del ejemplo anterior es un anillo conmutativo sin unidad.

Ejemplo 1.1.18. Sea $M_n(\mathbf{k})$ el conjunto de las matrices cuadradas de orden n con coeficientes en un cuerpo $\mathbf{k}$. Si $n > 1$, $M_n(\mathbf{k})$ con la suma y el producto usual de matrices es un anillo unitario no conmutativo.

Ejemplo 1.1.19. Sea n un número natural. En el conjunto $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, que llamaremos $\mathbf{Z}_n$ definimos las siguientes operaciones:

$$\begin{array}{rcl} \overline{m_1} + \overline{m_2} & = & \overline{r} \\ \overline{m_1} \cdot \overline{m_2} & = & \overline{s} \end{array}, \tag{1.1.19.1}$$

donde r es el resto (entre 0 y $n-1$) de dividir $m_1 + m_2$ entre n y s es el resto (entre 0 y $n-1$) de dividir $m_1 \cdot m_2$ entre n. Es claro que $+$ y $\cdot$ son operaciones internas en $\mathbf{Z}_n$. Con esas operaciones, $\mathbf{Z}_n$ es un anillo conmutativo unitario, que recibe el nombre de *anillo de restos módulo n*.

Comprobamos ahora algunas de las propiedades de la definición 0.1.2 (la asociativa de la suma, la distributiva, la existencia de elemento neutro de la suma, la existencia de elemento neutro del producto y la existencia de elemento opuesto) y dejamos la comprobación de las restantes como ejercicio. El elemento neutro de la suma es obviamente $\overline{0}$ y el del producto, $\overline{1}$. Dado $\overline{m} \in \mathbf{Z}_n$, el opuesto de $\overline{m}$ es $\overline{n-m}$.

Comprobamos la propiedad asociativa de la suma. Sean $\overline{x}, \overline{y}, \overline{z} \in \mathbf{Z}_n$. Debemos ver que

$$(\overline{x} + \overline{y}) + \overline{z} = (\overline{x} + \overline{y}) + \overline{z}. \tag{1.1.19.2}$$

Calculamos primero $(\overline{x} + \overline{y}) + \overline{z}$. Para calcular $\overline{x} + \overline{y}$ dividimos $x + y$ entre n como nos indica (1.1.19.1). Tenemos

$$x + y = q_1 n + r_1, \tag{1.1.19.3}$$

donde r_1 es un entero entre 0 y n_1. Entonces $\overline{x} + \overline{y} = \overline{r_1}$. Hallamos ahora $\overline{r_1} + \overline{z}$. Como nos indica (1.1.19.1), para ello hay que dividir $r_1 + z$ entre n:

$$r_1 + z = q_2 n + r_2, \tag{1.1.19.4}$$

donde r_2 es un entero entre 0 y n_1. De esto se sigue que $\overline{r_1} + \overline{z} = \overline{r_2}$. Tenemos pues que

$$(\overline{x} + \overline{y}) + \overline{z} = \overline{r_1} + \overline{z} = \overline{r_2}. \tag{1.1.19.5}$$

Calculamos por otra parte $\overline{x} + (\overline{y} + \overline{z})$. Razonando como antes dividimos $y + z$ entre n

$$y + z = q_3 n + r_3, \tag{1.1.19.6}$$

donde r_3 es un entero entre 0 y $n - 1$. Hallamos ahora $\overline{x} + \overline{r_3}$. Para ello hay que dividir $x + r_3$ entre n:

$$x + r_3 = q_4 n + r_4, \tag{1.1.19.7}$$

donde r_4 es un entero entre 0 y n_1. De esto se sigue que $\overline{x} + \overline{r_3} = \overline{r_4}$. Tenemos pues que

$$\overline{x} + (\overline{y} + \overline{z}) = \overline{x} + \overline{r_3} = \overline{r_4}. \tag{1.1.19.8}$$

De (1.1.19.3), (1.1.19.4) y la propiedad distributiva en $\mathbf{Z}$ se sigue

$$(x + y) + z = (q_1 + q_2)n + r_2. \tag{1.1.19.9}$$

De (1.1.19.6), (1.1.19.7) y la propiedad distributiva en $\mathbf{Z}$ se sigue

$$x + (y + z) = (q_3 + q_4)n + r_4. \tag{1.1.19.10}$$

La propiedad asociativa de la suma en $\mathbf{Z}$, la unicidad del resto, entre 0 y $n - 1$, de dividir entre n y las igualdades (1.1.19.9) y (1.1.19.10) implican que $r_2 = r_4$. Entonces, de (1.1.19.5) y (1.1.19.8) se sigue la igualdad (1.1.19.2) que queríamos demostrar.

Comprobamos la propiedad distributiva. Sean $\overline{x}, \overline{y}, \overline{z} \in \mathbf{Z}_n$. Debemos ver que

$$(\overline{x} + \overline{y})\overline{z} = \overline{xz} + \overline{yz}. \tag{1.1.19.11}$$

Calculamos primero $(\overline{x} + \overline{y})\overline{z}$. Para calcular $\overline{x} + \overline{y}$ dividimos $x + y$ entre n como nos indica (1.1.19.1). Tenemos

$$x + y = q_1 n + r_1, \tag{1.1.19.12}$$

donde r_1 es un entero entre 0 y n_1. Entonces $\overline{x} + \overline{y} = \overline{r_1}$. Hallamos ahora $\overline{r_1 z}$. Como nos indica (1.1.19.1), para ello hay que dividir $r_1 z$ entre n:

$$r_1 z = q_2 n + r_2, \tag{1.1.19.13}$$

donde r_2 es un entero entre 0 y n_1. De esto se sigue que $\overline{r_1 z} = \overline{r_2}$. Tenemos pues que

$$(\overline{x} + \overline{y})\overline{z} = \overline{r_1 z} = \overline{r_2}. \tag{1.1.19.14}$$

Calculamos por otra parte $\overline{xz} + \overline{yz}$. Razonando como antes dividimos xz e yz entre n

$$\begin{aligned} xz &= q_3 n + r_3 \\ yz &= q_4 n + r_4 \end{aligned} \tag{1.1.19.15}$$

donde r_3 y r_4 son enteros entre 0 y $n-1$. De aquí se sigue que $\overline{xz} = \overline{r_3}$ e $\overline{yz} = \overline{r_4}$. Dividimos ahora $r_3 + r_4$ entre n

$$r_3 + r_4 = q_5 n + r_5, \tag{1.1.19.16}$$

donde r_5 es un entero entre 0 y n_1. De esto se sigue que $\overline{r_3} + \overline{r_4} = \overline{r_5}$. Entonces

$$\overline{xz} + \overline{yz} = \overline{r_3} + \overline{r_4} = \overline{r_5}. \tag{1.1.19.17}$$

Entonces (1.1.19.14) y (1.1.19.17) nos dicen que para demostrar (1.1.19.11) hemos de comprobar que $\overline{r_2} = \overline{r_5}$. Para verlo razonamos así. Multiplicamos (1.1.19.12) y (1.1.19.13) por z y obtenemos

$$(x + y)z = q_1 zn + r_1 z = q_2 n + r_2. \tag{1.1.19.18}$$

Por otra parte de (1.1.19.15) y (1.1.19.16) obtenemos

$$xz + yz = (q_3 + q_4)n + (r_3 + r_4) = (q_3 + q_4 + q_5)n + r_5. \tag{1.1.19.19}$$

Por la propiedad distributiva en $\mathbf{Z}$, $(x + y)z = xz + yz$. Como el resto entre 0 y n_1 de dividir un entero entre n es único, (1.1.19.18) y (1.1.19.19) implican que $r_2 = r_5$, de donde $\overline{r_2} = \overline{r_5}$.

Ejercicio 1.1.20. (1) Demuestra la propiedad conmutativa de la suma y las propiedades asociativa y conmutativa del producto de $\mathbf{Z}_n$. Indicación: las propiedades conmutativas se siguen de manera inmediata de las propiedades conmutativas de $\mathbf{Z}$; para la propiedad asociativa del producto razona de manera similar a la comprobación de la propiedad asociativa de la suma y de la propiedad distributiva, usando en este caso que el resto de dividir xyz entre n son únicos.

(2) Demuestra que, dados $\overline{x}, \overline{y}, \overline{z} \in \mathbf{Z}_n$, $(\overline{x} + \overline{y}) + \overline{z} = \overline{s}$, donde s es el resto de dividir $x + y + z$ entre n.

(3) Demuestra que $(\overline{xy})\overline{z} = \overline{t}$, donde t es el resto de dividir xyz entre n.

Ejercicio 1.1.21. Escribe las tablas de la suma y del producto de los anillos $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_4$, $\mathbf{Z}_5$ y $\mathbf{Z}_6$. ¿Cuáles de ellos son cuerpos y cuáles no?

1.2 Divisores de cero. Unidades

Definición 1.2.1. Sea R un anillo.

(1) Sea r un elemento de R. Se dice que r es *divisor de cero por la izquierda* si $r \neq 0$ y existe $0 \neq s \in R$ tal que $rs = 0$. Se dice que r es un *divisor de cero por la derecha* si $r \neq 0$ y existe $0 \neq t \in R$ tal que $tr = 0$. Se dice que r es un *divisor de cero* si es divisor de cero a izquierda y derecha.

(2) Decimos que R es un *dominio de integridad* si es un anillo unitario no trivial que no tiene divisores de cero a izquierda ni a derecha (es claro que no tiene divisores de cero a izquierda si y solo si no los tiene a derecha). Dicho de otra forma, un anillo unitario R es dominio de integridad si $0 \neq 1$ y, para cualesquiera $r, s \in R$, $r, s \neq 0$, se tiene que $rs \neq 0$.

(3) Un elemento $r \in R$ se dice *nilpotente* si $r^n = 0$ para cierto $n \in \mathbf{N}$, $n \neq 0$.

Observación 1.2.2. Sean r, s, t elementos de $R, r \neq 0$. Si r no es divisor de cero por la izquierda (respectivamente, por la derecha) entonces $rs = rt$ implica $s = t$ (respectivamente $sr = tr$ implica $s = t$); es decir, podemos cancelar r en la ecuación anterior. En efecto, si r no es divisor de cero por la izquierda y $rs = rt$, entonces $0 = rs - rt = r(s - t)$ implica que $s - t = 0$ (el argumento si r no es divisor de cero por la derecha es análogo). En particular, si R es un dominio de integridad, para cualesquiera $r, s, t \in R, r \neq 0$ se tiene que $rs = rt$ implica $s = t$ y $sr = tr$ implica $s = t$.

Ejemplos 1.2.3. (1) Un elemento nilpotente no nulo es divisor de cero.

(2) Los elementos $\overline{2}$ de $\mathbf{Z}_6$ y $\overline{2}$ de $\mathbf{Z}_{12}$ son divisores de cero no nilpotentes.

(3) El elemento $\overline{2}$ de $\mathbf{Z}_8$ y el elemento $\overline{6}$ de $\mathbf{Z}_{12}$ son nilpotentes.

Ejemplos 1.2.4. (1) $\mathbf{Z}$ es un dominio de integridad, ya que el producto de dos enteros no nulo es distinto de 0.

(2) Calculando su tabla del producto se comprueba fácilmente que $\mathbf{Z}_2$, $\mathbf{Z}_3$ y $\mathbf{Z}_5$ son dominios de integridad. De hecho, si p un número primo, el anillo $\mathbf{Z}_p$ es un dominio de integridad. Esto se puede argumentar así. Si m_1, m_2 son números naturales menores que p, sus divisores primos también lo son por lo que $m_1 m_2$ no es múltiplo de p. Entonces el resto de dividir $m_1 m_2$ entre p es distinto de 0, por lo que $\overline{m_1 m_2} \neq 0$.[1]

[1] En este argumento hemos usado implícitamente la unicidad de la descomposición de un número natural como producto de números primos, hecho con el que te suponemos familiarizado. Veremos esta propiedad con detalle en la sección 3.3.

(3) Sea n un número compuesto (es decir, un número natural mayor que 1 no primo). El anillo $\mathbf{Z}_n$ no es un dominio de integridad, ya que, si n es compuesto, existen números naturales, ambos m_1, m_2 menores que n, tales que $n = m_1 m_2$. Como el resto de dividir n entre n es 0, tenemos $\overline{m_1} \cdot \overline{m_2} = \overline{m_1 m_2} = \overline{0}$, pero $\overline{m_1}, \overline{m_2} \neq 0$.

(4) Un cuerpo es un dominio de integridad (véase la observación 1.2.11 (4)).

Ejemplo 1.2.5. El anillo $M_n(\mathbf{k})$ no es un dominio de integridad y tiene elementos nilpotentes no nulos. Por ejemplo, en $M_2(\mathbf{k})$, se tiene que

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ y } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Proposición 1.2.6. *Un anillo unitario R es un dominio de integridad si y solo si $R[X]$ es un dominio de integridad.*

Demostración. Dejamos la demostración como ejercicio (ejercicio 9 de la hoja 1). □

Corolario 1.2.7. *Sea $\mathbf{k}$ un cuerpo.*

(1) El anillo $\mathbf{k}[X]$ es un dominio de integridad.

(2) Los anillos $\mathbf{Z}[X_1, \ldots, X_n]$ y $\mathbf{k}[X_1, \ldots, X_n]$ son dominios de integridad.

Definición 1.2.8. Sea R anillo unitario. Decimos que un elemento $r \in R$ tiene *inverso a izquierda* (respectivamente, *a derecha*) si existe $s \in R$, (respectivamente, $t \in R$) tal que $sr = 1$, (respectivamente, $rt = 1$). Decimos que $r \in R$ tiene *inverso* si existe $s \in R$ tal que $sr = rs = 1$.

Observación 1.2.9. (1) Si $r \in R$ tiene inverso a izquierda s e inverso a derecha t, entonces $s = t$, (ya que $s = s1 = s(rt) = (sr)t = 1t = t$); por tanto, r tiene inverso.

(2) Por lo anterior, si $r \in R$ tiene inverso, entonces dicho inverso es único, es decir, existe un único $s \in R$ tal que $sr = rs = 1$.

Definición 1.2.10. Sea R anillo unitario. A los elementos de R que tienen inverso los llamamos *unidades*. Si u es unidad, denotamos su inverso por u^{-1}. Denotamos al conjunto de las unidades de R por $U(R)$ o R^*.

Observación 1.2.11. (1) El conjunto $U(R)$ es un grupo respecto del producto de R. Si R es conmutativo, $U(R)$ es un grupo abeliano.

(2) Si u es unidad, $u \neq 0$, a menos que $R = 0$. En efecto, si $u = 0$, entonces $1 = uu^{-1} = 0 \cdot u^{-1} = 0$, pero estamos suponiendo que $0 \neq 1$ en R.

(3) Si u es una unidad de R entonces u no puede ser divisor de cero ni por la izquierda ni por la derecha. En efecto, sea u unidad y supongamos que sea divisor de cero por la izquierda, es decir, que exista $r \in R$ tal que $ur = 0$. Entonces $0 = u^{-1} \cdot 0 = u^{-1}(ur) = (u^{-1}u)r = 1 \cdot r = r$. El argumento para divisores de cero por la derecha es análogo. Por tanto $U(R)$ y el conjunto de divisores de cero de R, tanto por la izquierda como por la derecha, son disjuntos.

(4) Como consecuencia de (3), si $\mathbf{k}$ es un cuerpo, entonces $\mathbf{k}$ es un dominio de integridad. Sin embargo, existen dominios de integridad que no son cuerpos, como $\mathbf{Z}$ o $\mathbf{k}[X]$, donde $\mathbf{k}$ es un cuerpo (véanse los ejemplos 1.2.4 (1), 1.2.12 (1), (5) y la proposición 1.2.6)

Ejemplos 1.2.12. (1) Las unidades de $\mathbf{Z}$ son $U(\mathbf{Z}) = \{1, -1\}$.

(2) Si $\mathbf{k}$ es un cuerpo, sus unidades son $\mathbf{k}^* = \mathbf{k} \setminus \{0\}$. De hecho, un anillo conmutativo unitario R es un cuerpo si y solo si todo elemento no nulo de R es una unidad.

(3) Las unidades de $M_n(\mathbf{k})$ son las matrices con determinante no nulo.

(4) Las unidades de $\mathscr{C}(\mathbf{R}, \mathbf{R})$ son las funciones f tales que $f(x) \neq 0$ para todo $x \in \mathbf{R}$.

(5) Si $\mathbf{k}$ es un cuerpo, entonces las unidades de $\mathbf{k}[X]$ son los polinomios constantes no nulos (véase el ejercicio 9 de la hoja 1). Así pues, haciendo un pequeño abuso de la notación, podemos decir que $U(\mathbf{k}[X]) = U(\mathbf{k})$.

Ejercicio 1.2.13. Halla los divisores de cero y las unidades de $\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5$ y $\mathbf{Z}_6$ (indicación: revisa las tablas del producto de estos anillos).

1.3 Subanillos

Definición 1.3.1. Sea R un anillo con operaciones + y $\cdot$ y sea R' un subconjunto no vacío de R. Decimos que R' es un *subanillo* de R si para cualesquiera $r', s' \in R'$ se cumple

(1) $r' - s' \in R'$,

(2) $r' \cdot s' \in R'$.

Sea ahora R un anillo unitario y sea 1_R el elemento neutro del producto de R. Si además de (1) y (2) el conjunto R' cumple

(3) $1_R \in R'$

decimos que R' es un subanillo *unitario* de R.

Observación 1.3.2. (1) Si R' es un subanillo de R y restringimos las operaciones de R a R', entonces (1) y (2) implican que estas son operaciones internas de R'. En efecto, para el producto la afirmación se sigue inmediatamente de (2). En cuanto a la suma, como R es no vacío, existe un elemento $r' \in R'$ y (1) implica que el elemento neutro de la suma en R cumple $0_R = r' - r' \in R'$. Además, dado cualquier $r'_1 \in R'$, el opuesto de r'_1 en R cumple $-r'_1 = 0_R - r'_1 \in R'$, de nuevo por (1). Entonces (1) implica que, para cualesquiera $r'_1, r'_2 \in R'$, se cumple $r'_1 + r'_2 = r'_1 - (-r'_2) \in R'$.

Además, R' es un anillo respecto a dichas operaciones restringidas. En efecto, R' "hereda" las propiedades (1), (2), (5) y (6) de la definición 0.1.2 de las propiedades correspondientes de R y ya hemos visto que las propiedades (3) y (4) de la definición 0.1.2 se siguen de (1) de la definición 1.3.1.

(2) Si R es un anillo conmutativo y R' es un subanillo de R, por el mismo argumento R' es un anillo conmutativo. Sin embargo, existen subanillos conmutativos de anillos no conmutativos (véase el ejemplo 1.3.3 (4)).

(3) Si R es un anillo unitario y R' es un subanillo unitario de R, entonces R' es un anillo unitario.

(4) Si R es un dominio de integridad y R' es un subanillo de R, entonces R' es también un dominio de integridad ya que si existiera algún divisor de cero r' de R', entonces r' también sería divisor de cero de R. Sin embargo, un anillo que no es dominio de integridad puede contener subanillos que sí lo sean (véase el ejemplo 1.3.3 (4)).

(5) En particular, todo subanillo de un cuerpo es un dominio de integridad. ¡Sin embargo, un subanillo de un cuerpo no tiene por qué ser un cuerpo (véase el ejemplo 1.3.3 (1))!

Ejemplos 1.3.3. (1) Cada uno de los siguientes anillos son subanillos de aquellos que los contienen: $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$.

(2) El anillo $n\mathbf{Z}$ es un subanillo no unitario de $\mathbf{Z}$.

(3) Si R es un anillo, entonces R es un subanillo de $R[X]$.

(4) Sea $\mathbf{k}$ un cuerpo y sea D_n el conjunto de las matrices diagonales $n \times n$ con elementos en $\mathbf{k}$. Entonces D_n es un subanillo unitario de $M_n(\mathbf{k})$. Además, D_n es un cuerpo, por lo que, en particular, es un dominio de integridad y un anillo conmutativo.

(5) El anillo $\mathscr{C}(\mathbf{R}, \mathbf{R})$ de las funciones continuas de $\mathbf{R}$ en $\mathbf{R}$ es un subanillo unitario del anillo $\mathscr{A}(\mathbf{R}, \mathbf{R})$ de las funciones de $\mathbf{R}$ en $\mathbf{R}$.

(6) El anillo de las funciones de $\mathbf{R}$ en $\mathbf{R}$ con soporte compacto es un subanillo no unitario de $\mathscr{A}(\mathbf{R}, \mathbf{R})$.

1.4 Cuerpo de fracciones

Aunque estamos muy familiarizados con los números enteros, con los números racionales y con las operaciones definidas en estos dos conjuntos (de hecho, aprovechando esta familiaridad acabamos de afirmar, en el ejemplo 1.3.3 (1), que $\mathbf{Z}$ es un subanillo de $\mathbf{Q}$), conviene examinar con detenimiento cómo se construye el cuerpo $\mathbf{Q}$ a partir del anillo $\mathbf{Z}$.

Construcción del cuerpo de los números racionales.

En el conjunto $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ definimos la relación siguiente:

$$(a_1, a_2) \sim (b_1, b_2) \text{ si y solo si } a_1 b_2 - b_1 a_2 = 0. \tag{1.4.0.1}$$

La relación $\sim$ es una relación de equivalencia. En efecto, es inmediato ver que la relación $\sim$ cumple las propiedades reflexiva y simétrica. Comprobamos que la relación $\sim$ cumple también la propiedad transitiva: sean $(a_1, a_2), (b_1, b_2)$ y (c_1, c_2) de $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ tales que $(a_1, a_2) \sim (b_1, b_2)$ y $(b_1, b_2) \sim (c_1, c_2)$. Entonces

$$\begin{aligned} a_1 b_2 - b_1 a_2 &= 0 \\ b_1 c_2 - c_1 b_2 &= 0, \end{aligned}$$

de donde

$$0 = (a_1 b_2 - b_1 a_2) c_2 = a_1 b_2 c_2 - b_1 a_2 c_2 = a_1 b_2 c_2 - b_1 c_2 a_2 = a_1 b_2 c_2 - c_1 b_2 a_2 = (a_1 c_2 - c_1 a_2) b_2$$

y, cancelando b_2 (recuerda que $b_2 \neq 0$),

$$a_1 c_2 - c_1 a_2 = 0,$$

por lo que $(a_1, a_2) \sim (c_1, c_2)$.

Como la relación $\sim$ es una relación de equivalencia, podemos considerar el conjunto cociente, que es el conjunto formado por las clases de equivalencia de la relación $\sim$. A la clase de equivalencia de un elemento (a_1, a_2) de $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ la denotamos por a_1/a_2 o $\frac{a_1}{a_2}$, por lo que (1.4.0.1) quiere decir que

$$\frac{a_1}{a_2} = \frac{b_1}{b_2} \text{ si y solo si } a_1 b_2 - b_1 a_2 = 0$$

(recuerda que dos clases de equivalencia son iguales si y solo si sus representantes están relacionados). Así pues definimos el conjunto $\mathbf{Q}$ de los números racionales como el conjunto cociente de la relación $\sim$ de $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$.

Proposición 1.4.1. *Las operaciones $+$ y $\cdot$*

$$\frac{a_1}{a_2} + \frac{b_1}{b_2} := \frac{a_1 b_2 + b_1 a_2}{a_2 b_2}$$

$$\frac{a_1}{a_2} \cdot \frac{b_1}{b_2} := \frac{a_1 b_1}{a_2 b_2}$$

son operaciones internas en el conjunto $\mathbf{Q}$ *que acabamos de definir. El conjunto* $\mathbf{Q}$ *con las operaciones* $+$ *y* $\cdot$ *es un cuerpo y* $\mathbf{Z}$ *es un subanillo unitario de* $\mathbf{Q}$*.*

Demostración. Como hemos definido $\mathbf{Q}$ como un conjunto cociente y las operaciones $+$ y $\cdot$ usando representantes de las clases de equivalencia, lo primero que hay que ver es que $+$ y $\cdot$ están bien definidas, es decir, que no dependen de los representantes elegidos. Lo vemos para $+$ y dejamos como ejercicio la comprobación de que $\cdot$ está bien definida. Sean $a_1/a_2 = a_1'/a_2'$ y $b_1/b_2 = b_1'/b_2'$. Tenemos que ver que

$$\frac{a_1 b_2 + b_1 a_2}{a_2 b_2} = \frac{a_1' b_2' + b_1' a_2'}{a_2' b_2'}.$$

Esto es cierto ya que

$$(a_1 b_2 + b_1 a_2) a_2' b_2' = a_1 b_2 a_2' b_2' + b_1 a_2 a_2' b_2' = a_1 a_2' b_2 b_2' + b_1 b_2' a_2 a_2'$$

y, por ser $a_1/a_2 = a_1'/a_2'$ y $b_1/b_2 = b_1'/b_2'$, el último término es igual a

$$a_1' a_2 b_2 b_2' + b_1' b_2 a_2 a_2' = a_1' b_2' a_2 b_2 + b_1' a_2' a_2 b_2 = (a_1' b_2' + b_1' a_2') a_2 b_2$$

(observa que para este argumento hemos usado las propiedades asociativa y conmutativa del producto en $\mathbf{Z}$ y la propiedad distributiva).

Observamos a continuación que tanto la suma como el producto de elementos de $\mathbf{Q}$ son de nuevo elementos de $\mathbf{Q}$. Esto es cierto porque si a_1/a_2 y b_1/b_2 pertenecen a $\mathbf{Q}$, entonces $a_2, b_2 \neq 0$ (ya que $(a_1, a_2), (b_1, b_2) \in \mathbf{Z} \setminus \{0\}$)), por lo que $a_2 b_2 \neq 0$ (aquí estamos usando que $\mathbf{Z}$ es un dominio de integridad).

Vemos ahora que $\mathbf{Q}$ es un cuerpo. Comprobamos algunas de las propiedades de la definición y dejamos el resto como ejercicio. Para comprobar la propiedad asociativa de la suma tenemos que ver que si $a_1/a_2, b_1/b_2, c_1/c_2 \in \mathbf{Q}$, entonces

$$\left(\frac{a_1}{a_2} + \frac{b_1}{b_2}\right) + \frac{c_1}{c_2} = \frac{a_1}{a_2} + \left(\frac{b_1}{b_2} + \frac{c_1}{c_2}\right).$$

Para esto tenemos que ver que

$$\frac{(a_1 b_2 + b_1 a_2) c_2 + c_1 (a_2 b_2)}{(a_2 b_2) c_2} = \frac{a_1 (b_2 c_2) + (b_1 c_2 + c_1 b_2) a_2}{a_2 (b_2 c_2)},$$

para lo que hemos de comprobar que

$$((a_1 b_2 + b_1 a_2) c_2 + c_1 (a_2 b_2))(a_2 (b_2 c_2)) = (a_1 (b_2 c_2) + (b_1 c_2 + c_1 b_2) a_2)((a_2 b_2) c_2).$$

Esta última igualdad se sigue de las propiedades asociativa y conmutativa de la suma y del producto y de la propiedad distributiva de $\mathbf{Z}$. El resto de propiedades que ha de

cumplir **Q** para ser un anillo conmutativo unitario se comprueban de manera parecida y, finalmente, se siguen de las propiedades que tiene **Z** por ser un anillo conmutativo unitario. Por ejemplo, es muy sencillo ver que $0/1$ es el neutro de la suma de **Q**, que dado a_1/a_2 de **Q**, $(-a_1)/a_2$ es su elemento opuesto y que $1/1$ es el elemento neutro del producto en **Q**. Por último 7 comprobamos que la condición adicional necesaria para que **Q** sea un cuerpo: que todo a_1/a_2 no nulo es unidad. Ahora bien, se sigue de (1.4.0.1) que a_1/a_2 es no nulo si y solo si $a_1 \neq 0$. Por ello, a_2/a_1 es un elemento de **Q** y

$$\frac{a_1}{a_2}\frac{a_2}{a_1} = \frac{a_1a_2}{a_2a_1} = \frac{1}{1},$$

ya que $(a_1a_2)1 = 1(a_2a_1)$.
Para ver que **Z** es un subanillo de **Q**, identificamos cada número entero $a \in \mathbf{Z}$ con el número racional $a/1$. Es fácil ver que si $a, b \in \mathbf{Z}$,

$$\frac{a}{1} - \frac{b}{1} = \frac{a-b}{1},$$

que se identifica con el número entero $a - b$, y que

$$\frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1}.$$

Por otra parte como $1/1$ se identifica con $1 \in \mathbf{Z}$ podemos decir que el neutro del producto de **Q** está en **Z**. Por tanto, con la identificación hecha de los elementos de **Z** como números racionales podemos decir que **Z** es un subanillo unitario de **Q**. □

Observación 1.4.2. El último argumento de la demostración anterior, que usaba la identificación natural de los elementos de **Z** como números racionales, quizá no haya resultado del todo satisfactorio desde el punto de vista del rigor. La noción de *homomorfismo* de anillos, que veremos en el próximo tema, nos permitirá expresar el argumento de manera totalmente rigurosa.

Observación 1.4.3. Hemos definido **Q** haciendo una relación de equivalencia en $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$. Esto quiere decir que permitimos que el denominador de un número racional sea cualquier número entero excepto 0. ¿Por qué excluímos 0 como denominador? Si no lo hiciéramos, la relación (1.4.0.1) no sería una relación de equivalencia (¿ves por qué?).

Si nos fijamos en la construcción de **Q** a partir de **Z** y en los argumentos de la demostración de la proposición 1.4.1, vemos que las únicas propiedades de **Z** que hemos utilizado son las que se derivan de que **Z** sea un anillo conmutativo y un dominio de integridad. Esto quiere decir que la misma construcción será válida para cualquier anillo R que sea conmutativo y dominio de integridad. Podemos por tanto formular la siguiente proposición, que no demostramos, ya que su demostración sería exactamente igual

que lo argumentado en la construcción de **Q** y la demostración de la proposición 1.4.1, cambiando solo **Z** por R, **Q** por K, número entero por elemento de R y número racional por elemento de K. De hecho, podríamos haber demostrado primero la proposición 1.4.4 y haber obtenido la construcción de **Q** a partir de **Z** como un caso particular.

Proposición–Definición 1.4.4. *Sea R un anillo conmutativo que es además un dominio de integridad. En el conjunto $R \times (R \setminus \{0\})$ definimos la relación siguiente:*

(1.4.4.1) $$(a_1, a_2) \sim (b_1, b_2) \text{ si y solo si } a_1 b_2 - b_1 a_2 = 0.$$

(1) La relación $\sim$ es una relación de equivalencia.

(2) Al conjunto cociente de $\sim$ le llamaremos K. A la clase del elemento (a_1, a_2) de $R \times (R \setminus \{0\})$ la denotaremos a_1/a_2. Con esa notación (1.4.4.1) *se lee*

(1.4.4.2) $$\frac{a_1}{a_2} = \frac{b_1}{b_2} \text{ si y solo si } a_1 b_2 - b_1 a_2 = 0$$

(3) Las operaciones $+$ y $\cdot$

$$\frac{a_1}{a_2} + \frac{b_1}{b_2} = \frac{a_1 b_2 + b_1 a_2}{a_2 b_2}$$

$$\frac{a_1}{a_2} \cdot \frac{b_1}{b_2} = \frac{a_1 b_1}{a_2 b_2}$$

son operaciones internas en K.

(4) El conjunto K con las operaciones $+$ y $\cdot$ es un cuerpo y R es un subanillo unitario de K.

Observación 1.4.5. (1) La proposición 1.4.4 quiere decir que todo dominio de integridad conmutativo se puede "sumergir" dentro de un cuerpo. Por contra, si R no es un dominio de integridad, R no puede ser subanillo de ningún cuerpo (recuerda la observación 1.3.2 (5)).

(2) Dado un dominio de integridad conmutativo R, su cuerpo de fracciones K es el cuerpo "más pequeño" que lo contiene. Haremos más preciso este concepto en el tema siguiente. Por ahora nos quedamos con esta idea intuitiva: si queremos sumergir R en un cuerpo K' necesitamos que todos los elementos no nulos de R tengan inverso en K', por lo que, para todo $b \in R, b \neq 0$, $1/b$ debe estar en K'. Como el producto en K' es una operación interna y $R \subset K'$, para cualesquiera $a, b \in R, b \neq 0$, $a \cdot (1/b) = a/b$ debe pertenecer a K'. Por tanto $K \subset K'$.

Ejemplo 1.4.6. Sea **k** un cuerpo. El cuerpo de fracciones de $\mathbf{k}[X]$ (recuerda que, según el ejemplo 1.1.9 y la proposición 1.2.6, $\mathbf{k}[X]$ es un dominio de integridad conmutativo), que llamaremos $\mathbf{k}(X)$, es el conjunto de *funciones racionales*, que son las fracciones $f(X)/g(X)$, donde $f, g \in \mathbf{k}[X], g \neq 0$, equipado con la suma y el producto definidos en la proposición 1.4.4.

Tema 2

Ideales. Homomorfismos de anillos

Convenio. En lo que sigue solo estudiaremos anillos conmutativos unitarios. Por ello a partir de ahora para nosotros la palabra anillo significará anillo conmutativo unitario, a menos que digamos explícitamente otra cosa. Asimismo un subanillo será un subanillo unitario.

2.1 Ideales

Los *ideales* son los subconjuntos más importantes de un anillo. La noción de ideal surge a finales del siglo XIX en el contexto de la Teoría de Números y se convierte en el objeto central del Álgebra Conmutativa.[1]

Definición 2.1.1. Sea R un anillo. Un ideal I de R es un subconjunto no vacío de R que cumple las propiedades siguientes:

(1) para cualesquiera $x, y \in I$, se tiene $x + y \in I$;

(2) para cualesquiera $a \in R$, $x \in I$, se tiene $ax \in I$.

De la definición de ideal se deducen las siguientes propiedades:

Proposición 2.1.2. *Sea I un ideal de un anillo R.*

(1) Si $x \in I$, entonces $-x \in I$.

(2) $0_R \in I$.

(3) Si $\lambda_1, \ldots, \lambda_n \in R$, $x_1, \ldots, x_n \in I$, entonces $\lambda_1 x_1 + \cdots + \lambda_n x_n \in I$.

[1] El Álgebra Conmutativa es la rama del Álgebra que estudia los anillos conmutativos unitarios. La Geometría Algebraica y la Teoría Algebraica de Números se fundamentan en el Álgebra Conmutativa.

Demostración. Si $x \in I$, entonces $-x = (-1)x \in I$ por (2) de la definición 2.1.1. Esto demuestra (a). Como $I \neq \emptyset$, existe $x \in I$ y por (a), $-x \in I$, de donde $0_R = x + (-x) \in I$ por (1) de la definición 2.1.1. Esto prueba (b). Por último (c) se sigue de (1) y (2) de la definición 2.1.1 usando inducción sobre n.

□

Proposición 2.1.3. *Sea R un anillo y sea I un subconjunto de R no vacío. Entonces I es un ideal de R si y solo si para cualesquiera $x, y \in I$ y cualesquiera $\lambda, \mu \in R$, $\lambda x + \mu y \in I$.*

Demostración. Una de las implicaciones se sigue de la proposición 2.1.2, (c). Para la otra implicación, si $x, y \in I$ y $\lambda \in R$, entonces $x + y = 1 \cdot x + 1 \cdot y \in I$ y $\lambda x = \lambda \cdot x + 0 \cdot y \in I$. □

Observación 2.1.4. Sea R un anillo y sea I un subconjunto de R no vacío. Es fácil ver que I es un ideal de R si y solo si

(1′) para cualesquiera $x, y \in I$, se tiene $x - y \in I$;

(2) para cualesquiera $a \in R$, $x \in I$, se tiene $ax \in I$.

Ejemplos 2.1.5. (1) Sea R anillo. Entonces $\{0\}$ y R son ideales de R.

(2) Sea $n \in \mathbf{Z}$. Entonces $I = \{\lambda n \mid \lambda \in \mathbf{Z}\}$ es un ideal de $\mathbf{Z}$. En efecto, para cualesquiera $\lambda_1, \lambda_2 \in \mathbf{Z}$, se tiene $\lambda_1 n + \lambda_2 n = (\lambda_1 + \lambda_2)n \in I$, por lo que se cumple (1) de la definición 2.1.1 y para cualesquiera $\lambda, \mu \in \mathbf{Z}$, se tiene $\mu(\lambda n) = (\mu\lambda)n \in I$, por lo que se cumple (2) de la definición 2.1.1.

(3) Sea $R = \mathscr{C}(\mathbf{R}, \mathbf{R})$, el anillo de las funciones continuas de $\mathbf{R}$ en $\mathbf{R}$. Sea $p \in \mathbf{R}$. Entonces $I = \{f \in R \mid f(p) = 0\}$ es un ideal. En efecto, si $f_1, f_2 \in I$, entonces $(f_1 + f_2)(p) = f_1(p) + f_2(p) = 0 + 0 = 0$, por lo que $f_1 + f_2 \in I$ y se cumple (1) de la definición 2.1.1. Si $f \in I$, $g \in R$, entonces $(gf)(p) = g(p)f(p) = g(p)0 = 0$, por lo que $gf \in I$ y se cumple (2) de la definición 2.1.1.

Observación 2.1.6. Sea I un ideal de un anillo R. Las siguientes afirmaciones son equivalentes:

(1) $I = R$.

(2) $1 \in I$.

(3) I contiene una unidad de R.

En efecto, si $I = R$, entonces $1 \in I$, que es una unidad de R. Si I contiene una unidad u de R, entonces $1 = u^{-1}u \in I$, por lo que, para todo $x \in R$, $x = x \cdot 1 \in I$.

Ejemplo 2.1.7. El subconjunto S de $\mathbf{Z}$ formado por todos los números enteros impares no es un ideal. En efecto, no cumple ni (1) (la suma de dos números impares es par) ni (2) (el producto de un número par por un número impar es par) de la definición 2.1.1. Otra forma de ver que S no es un ideal es ver que no cumple la condición (2) de la proposición 2.1.2 (0 es par).

Intersección de ideales:

Proposición 2.1.8. *Sean I, J ideales de un anillo R. Entonces $I \cap J$ es un ideal de R.*

Demostración. Sean $x, y \in I \cap J$. Entonces $x, y \in I$, $x, y \in J$. Por ser I, J ideales se tiene que $x + y \in I, x + y \in J$, de donde $x + y \in I \cap J$. De igual manera, si $a \in R$, $x \in I \cap J$, entonces $x, y \in I$, $x, y \in J$. Por ser I, J ideales se tiene que $ax \in I, ax \in J$, de donde $ax \in I \cap J$. Por tanto $I \cap J$ cumple (1) y (2) de la definición 2.1.1. □

Observación 2.1.9. Dada una colección finita de ideales o, incluso, dada una colección arbitraria de ideales, se puede realizar esencialmente el mismo argumento de la demostración de la proposición 2.1.8. Así pues, la intersección de una colección arbitraria de ideales es un ideal.

Ideal generado por un conjunto:

Como nos muestra el ejemplo 2.1.7, no todo subconjunto no vacío de un anillo es un ideal. Por eso es interesante, dado un subconjunto arbitrario Σ de un anillo R, considerar el ideal más pequeño de R que contiene a Σ:

Definición 2.1.10. Sea R un anillo y sea Σ un subconjunto de R.

(1) El *ideal generado por* Σ, que denotaremos por (Σ), es el ideal que consiste en la intersección de todos los ideales de R que contienen a Σ (si $\Sigma = \{a_1, \ldots, a_n\}$ es un conjunto finito, escribiremos $(a_1, \ldots, a_n)$ en vez de $(\{a_1, \ldots, a_n\})$).

(2) Si $I = (\Sigma)$, diremos que Σ es un *sistema de generadores* de I.

(3) Si I posee un sistema de generadores finito diremos que I está *finitamente generado*.

Ejemplos 2.1.11. Sea R anillo.

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

(2) $(1) = R$. Además, se sigue de la observación 2.1.6 que $a \in R$ cumple $(a) = R$ si y solo si a es una unidad de R.

Como consecuencia de la observación 2.1.6 y del ejemplo 2.1.11 (2) tenemos el siguiente resultado:

Proposición 2.1.12. *Un anillo R es un cuerpo si y solo si los únicos ideales de R son (0) y (1).*

Demostración. Si I es un ideal de R, $I \neq (0)$, entonces existe $a \in I$, $a \neq 0$. Si R es un cuerpo, entonces a es una unidad de R, por lo que, por la observación 2.1.6, $I = (1)$, así que R solo tiene dos ideales, (0) y (1).
Sea ahora R un anillo cuyos únicos ideales son (0) y (1). Sea $a \in R$, $a \neq 0$. Entonces el ideal $(a) \neq (0)$, por lo que $(a) = (1)$. Por el ejemplo 2.1.11 (2), a es una unidad de R. □

Proposición 2.1.13. *El ideal generado por Σ es el ideal "más pequeño" que contiene a Σ, es decir, si llamamos $J = (\Sigma)$:*

(i) J es un ideal;

(ii) $\Sigma \subset J$;

(iii) si I es un ideal y $\Sigma \subset I$, entonces $J \subset I$.

Un ideal que cumple (ii) y (iii) es único.

Demostración. El apartado (i) se sigue de la observación 2.1.9. El apartado (ii) se sigue de la definición de (Σ). Vemos ahora que se cumple (iii). Si $\Sigma \subset I$ e I es un ideal, entonces I es uno de los ideales que está en la intersección que da lugar a (Σ), por lo que $(\Sigma) \subset I$.
Veamos ahora la unicidad del ideal generado por Σ. Sean J_1 y J_2 dos ideales que cumplen (ii) y (iii). Como J_2 cumple (ii) y J_1 cumple (iii), tenemos $J_1 \subset J_2$. Recíprocamente, como J_1 cumple (ii) y J_2 cumple (iii), tenemos $J_2 \subset J_1$. □

Proposición 2.1.14. *Sea R un anillo y sean $a_1, \dots, a_n \in R$. Entonces*

$$(a_1, \dots, a_n) = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_1, \dots, \lambda_n \in R\}.$$

Demostración. Llamemos J a $\{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_1, \dots, \lambda_n \in R\}$ y veamos que J cumple (i), (ii), (iii) de la proposición 2.1.13; en ese caso, por la unicidad enunciada en la proposición 2.1.13, tendremos que $J = (a_1, \dots, a_n)$.
Vemos primero que J es un ideal usando la proposición 2.1.3. Sean

$$\lambda, \mu, \lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n \in R.$$

Entonces, dados dos elementos cualesquiera $\lambda_1 a_1 \cdots + \lambda_n a_n$ y $\mu_1 a_1 \cdots + \mu_n a_n$ de J, tenemos que

$$\begin{gathered}\lambda(\lambda_1 a_1 \cdots + \lambda_n a_n) + \mu(\mu_1 a_1 \cdots + \mu_n a_n) = \\ (\lambda\lambda_1)a_1 \cdots + (\lambda\lambda_n)a_n + (\mu\mu_1)a_1 \cdots + (\mu\mu_n)a_n = \\ (\lambda\lambda_1 + \mu\mu_1)a_1 \cdots + (\lambda\lambda_n + \mu\mu_n)a_n\end{gathered}$$

también está en J.
Para ver que J cumple (ii) de la proposición 2.1.13 basta escribir, para todo $i \in \{1, \dots, n\}$, a_i como $a_i = 0 \cdot a_1 + \cdots + 1 \cdot a_i + \cdots + 0 \cdot a_n$.
Por último, si $\{a_1, \dots, a_n\} \subset I$ e I es un ideal, entonces, para cualesquiera $\lambda_1, \dots, \lambda_n \in R$, se tiene, por el apartado (3) de la proposición 2.1.2, que $\lambda_1 a_1 + \cdots \lambda_n a_n \in I$, de donde $J \subset I$.
EN CLASE deducir que J es la intersección de todos los ideales que contienen a Σ □

Observación 2.1.15. Usando esencialmente los mismos argumentos que en la demostración de la proposición 2.1.14 se ve que, si Σ es un subconjunto arbitrario no vacío de R, no necesariamente finito, entonces

$$(\Sigma) = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_1, \dots, \lambda_n \in R, a_1, \dots, a_n \in \Sigma\}.$$

Ejemplos 2.1.16. (1) Sea $n \in \mathbf{Z}$. El ideal (n) es el subconjunto de $\mathbf{Z}$ formado por los múltiplos de n.

(2) Los ideales $(12, 28)$ y (4) de $\mathbf{Z}$ son iguales. En efecto, los elementos de $(12, 28)$ son de la forma $\lambda \cdot 12 + \mu \cdot 28$ para algún λ y algún μ de $\mathbf{Z}$. Como $\lambda \cdot 12 + \mu \cdot 28 = (\lambda \cdot 3 + \mu \cdot 7) \cdot 4$, vemos que $(12, 28) \subset (4)$.

Vemos que $4 = 1 \cdot 28 + (-2) \cdot (12)$, de donde, para todo $\lambda \in \mathbf{Z}$, $\lambda \cdot 4 = \lambda \cdot 28 + (-2\lambda) \cdot (12)$, por lo que $(4) \subset (12, 28)$.

Más adelante veremos que, si n_1, n_2 son enteros no nulos y m es el máximo común divisor de n_1 y n_2, entonces $(m) = (n_1, n_2)$.

(3) Sea $\mathbf{k}$ cuerpo. El conjunto de polinomios de $R = \mathbf{k}[X, Y]$ que es anulan al sustituir X por 0 e Y por 0 es el ideal generado por X e Y. En efecto, sea f un polinomio cualquiera de R y sea a_{00} su término independiente. Si $f(0, 0) = 0$, entonces a_{00}, por lo que los términos de f son, o bien múltiplos de X, o bien múltiplos de Y. Así f se puede escribir (no de forma única) como $f = f_1 \cdot X + f_2 \cdot Y$, para ciertos polinomios f_1, f_2 de R.

Recíprocamente, si $f = f_1 \cdot X + f_2 \cdot Y$ para ciertos polinomios f_1, f_2 de R, entonces $f(0, 0) = f_1(0, 0) \cdot 0 + f_2(0, 0) \cdot 0 = 0$, por lo que lo que los polinomios de (X, Y) se anulan al sustituir X por 0 e Y por 0.

Casi todos los ejemplos de anillos que hemos visto y veremos cumplen la propiedad de que todos sus ideales están finitamente generados.[2] Sin embargo, existen anillos con ideales que no están finitamente generados, como muestra el siguiente ejemplo:

Ejemplo 2.1.17. Sea $\mathbf{k}$ un cuerpo y sea

$$R = \bigcup_{n=1}^{\infty} \mathbf{k}[X_1, \ldots, X_n].$$

No es difícil ver que R es un anillo con respecto a la suma y producto obvios. Consideramos

$$I = \bigcup_{n=1}^{\infty} (X_1, \ldots, X_n),$$

donde $(X_1, \ldots, X_n)$ es el ideal generado en R por $X_1, \ldots, X_n$. Por el lema 3.3.4, I es un ideal de R. Dejamos como ejercicio comprobar que I es el ideal de R generado por el conjunto $\{X_1, X_2, \ldots, X_n, \ldots\}$ y que I no está finitamente generado.

[2] Esos anillos reciben el nombre de anillos *noetherianos* en honor a Emmy Noether.

Suma de ideales:

Observación 2.1.18. La unión de ideales *no* es en general un ideal. Por ejemplo, si $\mathbf{k}$ es un cuerpo y $R = \mathbf{k}[X, Y]$, el conjunto $(X) \cup (Y)$ no es un ideal, ya que dicho conjunto está formado por aquellos polinomios de $\mathbf{k}[X, Y]$ cuyos términos son o bien todos múltiplos de X o bien todos múltiplos de Y. Si $(X) \cup (Y)$ fuera un ideal, $X + Y$ debería estar en él, pero por lo que acabamos de decir no es así.

Ejercicio 2.1.19. Sea R un anillo y sean I, J ideales de R. Demuestra que $I \cup J$ es un ideal de R si y solo si $I \subset J$ o $J \subset I$.

Teniendo en cuenta la observación 2.1.18 y el ejercicio 2.1.19, tiene sentido considerar el ideal más pequeño que contiene a $I \cup J$, es decir, el ideal generado por $I \cup J$:

Definición 2.1.20. Sea R un anillo y sean I, J ideales de R. El *ideal suma* de I y J, que denotamos por $I + J$, es el ideal generado por $I \cup J$.

Proposición 2.1.21. *Sean I y J dos ideales de un anillo R. Entonces $I + J = \{a + b \mid a \in I, b \in J\}$.*

Demostración. Llamamos $K = \{a + b \mid a \in I, b \in J\}$. Vemos primero que K es un ideal. Sean $a_1, a_2 \in I$, $b_1, b_2 \in J$ y $\lambda_1, \lambda_2 \in R$. En ese caso

$$\lambda_1(a_1 + b_1) + \lambda_2(a_2 + b_2) = (\lambda_1 a_1 + \lambda_2 a_2) + (\lambda_1 b_1 + \lambda_2 b_2)$$

pertenece a K, ya que $\lambda_1 a_1 + \lambda_2 a_2 \in I$ y $\lambda_1 b_1 + \lambda_2 b_2 \in J$.
Vemos ahora que $(I \cup J) \subset K$. Si $a \in I$, entonces $a = a + 0$, que pertenece a K porque $0 \in J$. Análogamente, si $b \in J$, entonces $b = 0 + b$, que pertenece a K porque $0 \in I$. Entonces $I \subset K$ y $J \subset K$, de donde $I \cup J \subset K$. La proposición 2.1.13 implica que $(I \cup J) \subset K$.
Finalmente vemos que $K \subset (I \cup J)$. Sea $a + b \in K$, con $a \in I$ y $b \in J$. Como $a \in I \subset I \cup J \subset (I \cup J)$ y $b \in J \subset I \cup J \subset (I \cup J)$ y como $(I \cup J)$ es un ideal, tenemos que $a + b \in (I \cup J)$. □

Ejemplos 2.1.22. (1) Sea $\mathbf{k}$ cuerpo y $R = \mathbf{k}[X, Y]$. Entonces $(X) + (Y) = (X, Y)$.

(2) Sea $\mathbf{k}$ cuerpo y $R = \mathbf{k}[X]$. Entonces $(X) + (X - 1) = (1)$.

(3) En $\mathbf{Z}$, $(12) + (28) = (12, 28) = (4)$.

Más adelante veremos que, si n_1, n_2 son enteros no nulos y m es el máximo común divisor de n_1 y n_2, entonces $(m) = (n_1) + (n_2)$.

Producto de ideales:

Definición 2.1.23. Sean I, J dos ideales de un anillo R. El *ideal producto* de I y J, que denotamos $I \cdot J$, es el ideal generado por el conjunto $\{a \cdot b \mid a \in I, b \in J\}$.

Como muestra el siguiente ejercicio, $\{a \cdot b \mid a \in I, b \in J\}$ no es en general un ideal de R. Por eso es necesario considerar el ideal generado por $\{a \cdot b \mid a \in I, b \in J\}$ para definir el ideal producto.

Ejercicio 2.1.24. Sea $\mathbf{k}$ cuerpo y sea $R = \mathbf{k}[X, Y, Z, W]$ el anillo de polinomios en cuatro variables con coeficientes en $\mathbf{k}$. Sean $I = (X, Y)$ y $J = (Z, W)$. Demuestra que $\{a \cdot b \mid a \in I, b \in J\}$ no es un ideal de R.
Indicación: demuestra que $XZ+YW$ no se puede escribir como producto de un polinomio de I y otro polinomio de J.

Ideales coprimos:

Vemos ahora la relación entre producto e intersección de ideales.

Definición 2.1.25. Sea R un anillo y sean I y J dos ideales de R. Decimos que I y J son *comaximales*, *coprimos* o *primos entre sí* si $I + J = (1)$.

Proposición 2.1.26. *Sea R un anillo y sean I y J dos ideales de R.*

(1) $IJ \subset I \cap J$.

(2) Si I y J son coprimos, entonces $IJ = I \cap J$.

Demostración. Dado un elemento x de I y un elemento y de J, su producto xy está en $I \cap J$. Como el ideal IJ está generado por los elementos de la forma xy, donde $x \in I$ e $y \in J$ e $I \cap J$ es un ideal, IJ está contenido en $I \cap J$. Esto demuestra (1).

Para demostrar (2) basta entonces con ver que, si I y J son coprimos, entonces $I \cap J \subset IJ$. Como I y J son coprimos, existen $x \in I$, $y \in J$ tales que $1 = x + y$. Si $z \in I \cap J$, entonces $z = z \cdot 1 = zx + zy$. Como zx y zy están en IJ, z también lo está. □

2.2 Anillo cociente

Ya conocemos el concepto de conjunto cociente por una relación de equivalencia. En Álgebra nos interesa ir un paso más allá: si un conjunto está equipado con una determinada estructura algebraica, queremos poder dotar al conjunto cociente de esa misma estructura algebraica de una manera natural. Este tipo de construcción también aparece en Álgebra Lineal: si V es un espacio vectorial, ciertos conjuntos cocientes de V son también espacios vectoriales, de una manera que es compatible con la estructura espacio vectorial de V. Los conjuntos cocientes que tienen estructura de espacio vectorial son los de aquellas relaciones de equivalencia definidas a partir de subconjuntos de V adecuados, los subespacios vectoriales.

En nuestro caso queremos, dado un anillo R, considerar cocientes suyos que tengan una estructura de anillo compatible con la de R. Para eso consideramos relaciones de equivalencia definidas por subconjuntos adecuados de R. En este caso los subconjuntos adecuados son los ideales de R.

Proposición 2.2.1. *Sea I un ideal de un anillo R. La relación $\sim$ definida, para cualesquiera $x, y \in R$ por*

$$x \sim y \quad \textit{si y solo si} \quad x - y \in I,$$

es una relación de equivalencia.

Demostración. Vemos que $\sim$ cumple las propiedades reflexiva, simétrica y transitiva. Sean $x, y, z \in R$.
Propiedad reflexiva: $x - x = 0 \in I$, por el apartado (2) de la proposición 2.1.2, por lo que $x \sim x$.
Propiedad simétrica: Si $x \sim y$, entonces $x - y \in I$. Por el apartado (1) de la proposición 2.1.2 $y - x = -(x - y) \in I$, por lo que $y \sim x$.
Propiedad transitiva. Si $x \sim y$ e $y \sim z$, entonces $x - y \in I$ e $y - z \in I$. Por el apartado (1) de la definición 2.1.1, $x - z = (x - y) + (y - z) \in I$, por lo que $x \sim z$. □

Observación 2.2.2. La relación de equivalencia definida en la proposición 2.2.1 en el anillo R por el ideal I de R es totalmente análoga a la relación inducida en un espacio vectorial V por un subespacio vectorial W de V. La razón es que I y W son *subgrupos*, respectivamente, de los grupos abelianos $(R, +)$ y $(V, +)$. Como veremos cuando estudiemos grupos esto va a permitir que los conjuntos cocientes respectivos tengan estructura de grupos abelianos. El cociente de V tendrá además una operación externa que lo convertirá en espacio vectorial. El cociente de R tendrá además una operación interna que lo convertirá en un anillo.

Definición 2.2.3. Sea I un ideal del anillo R y sea $\sim$ la relación de equivalencia inducida por I definida en la proposición 2.2.1.

(1) Dado $x \in R$, denotamos por $\overline{x}$ a la clase de equivalencia de x respecto de $\sim$, es decir,

$$\overline{x} := \{y \in R \mid y \sim x\} = \{y \in R \mid y - x \in I\}.$$

(2) A veces a la clase de x la denotaremos también $x + I$, sobre todo cuando trabajemos con relaciones de equivalencia inducidas por varios ideales y el uso de la notación de (1) produzca ambigüedad. La notación $x + I$ evoca el hecho de que la clase de x es en realidad el subconjunto $\{x + z \mid z \in I\}$.

(3) Denotamos por R/I al conjunto cociente de $\sim$, es decir,

$$R/I := R/\!\sim = \{\overline{x} \mid x \in R\}.$$

Proposición 2.2.4. *Sea I un ideal del anillo R y sean $x, y \in R$. Definimos*

(i) $\overline{x} + \overline{y} := \overline{x + y}$;

(ii) $\overline{x} \cdot \overline{y} := \overline{x \cdot y}$.

En ese caso

(1) la suma + y el producto · definidos en (i) y (ii) son operaciones internas de R/I bien definidas;

(2) el conjunto cociente R/I con las operaciones + y · definidas en (i) y (ii) es un anillo.

Demostración. Primero hay que ver que + y · están bien definidas en el conjunto cociente. Esta comprobación es necesaria porque estamos definiéndolas usando *representantes* de las clases y debemos ver que nuestras definiciones no dependen de los representantes elegidos.

Concretamente para + debemos ver que si $\overline{x} = \overline{x'}$ e $\overline{y} = \overline{y'}$, entonces $\overline{x+y} = \overline{x'+y'}$ o, lo que es mismo, que si $x \sim x'$ e $y \sim y'$, entonces $x + y \sim x' + y'$. Si $x \sim x'$ e $y \sim y'$, entonces $x - x' \in I$ e $y - y' \in I$, de donde $(x + y) - (x' + y') = (x - x') + (y - y') \in I$, por el apartado (1) de la definición 2.1.1.

Para · debemos ver que si $\overline{x} = \overline{x'}$ e $\overline{y} = \overline{y'}$, entonces $\overline{x \cdot y} = \overline{x' \cdot y'}$ o, lo que es mismo, que si $x \sim x'$ e $y \sim y'$, entonces $xy \sim x'y'$. Si $x \sim x'$ e $y \sim y'$, entonces $x - x' \in I$ e $y - y' \in I$, de donde $xy - x'y' = xy - x'y + x'y - x'y' = y(x - x') + x'(y - y)' \in I$, por el apartado (3) de la proposición 2.1.2.

Demostramos ahora (2). Necesitamos ver que la suma y el producto definidos en R/I cumplen las ocho propiedades de la definición de anillo conmutativo con unidad. Como vamos a ver, estas propiedades vienen "heredadas" de las ocho propiedades que cumplen la suma y el producto de R. Comprobamos algunas de ellas y dejamos el resto como ejercicio.

Por ejemplo, para ver la propiedad asociativa de la suma debemos asegurarnos que, dados $x, y, z \in R$, se tiene $(\overline{x} + \overline{y}) + \overline{z} = \overline{x} + (\overline{y} + \overline{z})$. Esta igualdad es cierta porque, por una parte,

$$(\overline{x} + \overline{y}) + \overline{z} = \overline{x+y} + \overline{z} = \overline{(x+y)+z}$$

y, por otra parte,

$$\overline{x} + (\overline{y} + \overline{z}) = \overline{x} + \overline{y+z} = \overline{x + (y+z)}.$$

Como $(x + y) + z = x + (y + z)$ por la propiedad asociativa de la suma en R, se tiene $(\overline{x} + \overline{y}) + \overline{z} = \overline{x} + (\overline{y} + \overline{z})$ como queríamos.

La propiedad conmutativa de la suma se comprueba de manera análoga.

El elemento neutro de la suma en R/I es $\overline{0_R}$ ya que, dado $x \in R$, se tiene $\overline{x} + \overline{0_R} = \overline{x + 0_R} = \overline{x}$, ya que $x + 0_R = x$.

Dado $x \in R$, es claro que el elemento opuesto de $\overline{x}$ con respecto a la suma es la clase de $-x$ (donde $-x$ es el opuesto de x en R); es decir, el opuesto de $\overline{x}$ es $\overline{-x}$ o, dicho de otra forma, $-\overline{x} = \overline{-x}$.

Es claro que el elemento neutro del producto en R/I es $\overline{1_R}$.

El resto de propiedades (asociativa del producto, conmutativa del producto y distributiva) se comprueban de manera análoga y las dejamos como ejercicio. □

Ejemplo 2.2.5. Sea I un ideal de un anillo R. El anillo cociente R/I es el anillo nulo si y solo si $I = (1)$.

Ejemplo 2.2.6. Sea $R = \mathbf{Z}$, sea $n \in \mathbf{Z}$ y sea $I = (n)$. La relación $\sim$ inducida por I es la siguiente: dados $m_1, m_2 \in \mathbf{Z}$, $m_1 \sim m_2$ si y solo si $m_1 - m_2 \in (n)$, es decir, si y solo si $m_1 - m_2$ es múltiplo de n.

Por ejemplo, si $n = 7$, el conjunto cociente $\mathbf{Z}/(7)$ es

$$\mathbf{Z}/(7) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}.\ ^{3}$$

Esto es así porque, dado cualquier $m \in \mathbf{Z}$ su resto de dividir por 7 es $0, 1, 2, 3, 4, 5$ o 6, es decir, existen $q \in \mathbf{Z}$ y $r \in \{0, 1, 2, 3, 4, 5, 6\}$ tales que $m = qn + r$, de donde $m - r$ es múltiplo de n, por lo que $m \sim r$ y $\overline{m} = \overline{r}$. Por otra parte los elementos $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$ de $\mathbf{Z}/(7)$ son todos distintos entre sí: por ejemplo, $\overline{3} \neq \overline{5}$, ya que $3 \not\sim 5$, pues $5 - 3$ no es múltiplo de 7.

A modo de ejemplo, calculamos la suma, el producto y los opuestos de un par de elementos de $\mathbf{Z}/(7)$, $\overline{4}$ y $\overline{5}$. La suma de $\overline{4}$ y $\overline{5}$ es $\overline{2}$, ya que $\overline{4} + \overline{5} = \overline{9} = \overline{2}$, porque $9 \sim 2$ al ser $9 - 2$ múltiplo de 7.

El producto de $\overline{4}$ y $\overline{5}$ es $\overline{6}$, ya que $\overline{4} \cdot \overline{5} = \overline{20} = \overline{6}$, porque $20 \sim 6$ al ser $20 - 6$ múltiplo de 7.

El opuesto de $\overline{4}$ es $\overline{3}$, ya que $\overline{4} + \overline{3} = \overline{7} = \overline{0}$. Visto de otra forma, $\overline{-4} = \overline{3}$, ya que $-4 \sim 3$, puesto que $-4 - 3$ es múltiplo de 7. De igual manera, el opuesto de $\overline{5}$ es $\overline{2}$.

Ejercicio 2.2.7. Calcula las tablas de la suma y del producto de $\mathbf{Z}/(7)$. Compara estas con las del anillo de restos $\mathbf{Z}_7$, no solo las tablas en sí sino la forma de hacer los cálculos en ambos casos.

Observación 2.2.8. La relación $\sim$ del ejemplo 2.2.6 es la misma que la relación de *congruencia módulo m* descrita en el ejemplo A.1, ya que $m_1 - m_2$ es divisible por n si y solo si m_1 y m_2 tienen el mismo resto, entre 0 y $n - 1$, al dividir por n.

Ejercicio 2.2.9. Sea $R = \mathbf{R}[X]$ y sea $I = (X - 3)$. Sean $f, g \in \mathbf{R}[X]$. Demuestra que los elementos $\overline{f}$ y $\overline{g}$ de R/I son iguales si y solo si los polinomios f y g toman el mismo valor al ser evaluados en 3.

2.3 Homomorfismos de anillos

En Álgebra, cuando estamos estudiando aplicaciones entre objetos dotados con una misma estructura algebraica, nos interesan aquellas que respetan la estructura. Así, en

[3] No confundas la notación empleada aquí para los elementos del anillo cociente $\mathbf{Z}/(n)$ con la de los elementos del anillo de restos $\mathbf{Z}_n$ (ejemplo 1.1.19). En la proposición 3.2.13 veremos en detalle que $\mathbf{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ y en el corolario 3.2.14 veremos que hay un *isomorfismo* natural entre ambos anillos por lo que la aparente ambigüedad en la notación no es tanta.

Álgebra Lineal, las aplicaciones interesantes entre espacios vectoriales son las aplicaciones lineales u homomorfismos entre espacios vectoriales, pues son las que respectan la suma y el producto por escalares. Ahora las aplicaciones que nos interesan son las que respetan la estructura de anillo:

Definición 2.3.1. Sean R y S anillos y sea $\varphi : R \longrightarrow S$ una aplicación entre R y S. Decimos que φ es un *homomorfismo de anillos* si para cualesquiera $x, y \in R$,

(1) $\varphi(x + y) = \varphi(x) + \varphi(y)$;

(2) $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$;

(3) $\varphi(1_R) = 1_S$.

Proposición 2.3.2. *Sea $\varphi : R \longrightarrow S$ un homomofismo entre dos anillos R y S.*

(1) $\varphi(0_R) = 0_S$.

(2) Dado $x \in R$, $\varphi(-x) = -\varphi(x)$.

(3) Si u es una unidad de R, entonces $\varphi(u)$ es unidad de S y $\varphi(u^{-1}) = \varphi(u)^{-1}$.

Demostración. (1): Llamemos $z = \varphi(0_R)$. Por la propiedad (1) de la definición 2.3.1, $z = \varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R) = z + z$. Sumando $-z$ a ambos lados obtenemos $\varphi(0_R) = z = 0_S$.
(2): Por el apartado (1), $\varphi(0_R) = 0_S$. Por la propiedad (1) de la definición 2.3.1, $0_S = \varphi(0_R) = \varphi(x + (-x)) = \varphi(x) + \varphi(-x)$, de donde $\varphi(-x) = -\varphi(x)$.
(3): Por la propiedad (3) de la definición 2.3.1, $\varphi(1_R) = 1_S$. Si u es una unidad de R, se sigue de la propiedad (2) de la definición 2.3.1 que $\varphi(1_R) = \varphi(u \cdot u^{-1}) = \varphi(u) \cdot \varphi(u^{-1})$, de donde $\varphi(u)$ es una unidad de S y el inverso de $\varphi(u)$ es $\varphi(u^{-1})$. □

Observación 2.3.3. Al contrario que la propiedad (1) de la proposición 2.3.2, la propiedad (3) de la definición 2.3.1 no es superflua, ya que no se sigue de las propiedades (1) y (2) de dicha definición. Por ejemplo, si R y S son anillos y $S \neq 0$, la aplicación

$$\begin{array}{rccc} \varphi : & R & \longrightarrow & S \\ & x & \mapsto & 0_S \end{array}$$

cumple (1) y (2) de la definición 2.3.1 pero $\varphi(1_R) = 0_S \neq 1_S$.
Otro ejemplo menos trivial es el siguiente. Sean R y S dos anillos y sea $R \times S$ el anillo producto cartesiano definido en el ejercicio (3) de la hoja 1. Las aplicaciones

$$\begin{array}{rccc} \varphi : & R \times S & \longrightarrow & R \times S \\ & (x, z) & \mapsto & (x, 0_S) \end{array}$$

y

$$\begin{array}{rccc} \psi : & R \times S & \longrightarrow & R \times S \\ & (x, z) & \mapsto & (0_R, z) \end{array}$$

cumplen (1) y (2) de la definición 2.3.1 pero $\varphi((1_R, 1_S)) = (1_R, 0_S)$ y $\psi((1_R, 1_S)) = (0_R, 1_S)$, por lo que no cumplen la propiedad (3) de la definición 2.3.1.
Sin embargo, como nuestros anillos son unitarios, es razonable y conveniente que los homomorfismos entre ellos transformen el neutro del producto en el neutro del producto. Por lo visto en los ejemplos anteriores, para conseguir esto es por lo que es necesario incluir la propiedad (3) en la definición 0.1.2.

Definición 2.3.4. Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos. Si φ es una aplicación biyectiva (es decir, inyectiva y sobreyectiva) decimos que φ es un *isomorfismo de anillos*. Si existe un isomorfismo de anillos entre dos anillos R y S decimos que R y S son anillos *isomorfos*.

Recordemos que una aplicación biyectiva $\varphi : A \longrightarrow B$ entre dos conjuntos tiene una (única) *aplicación inversa*, que se denota φ^{-1}, que consiste en

$$\begin{array}{rccc} \varphi^{-1}: & B & \longrightarrow & A \\ & b & \mapsto & a, \end{array} \tag{2.3.4.1}$$

donde a es el único elemento de A que cumple $\varphi(a) = b$. La aplicación φ^{-1} está caracterizada por

$$\varphi^{-1} \circ \varphi = \mathrm{id}_A \quad \text{y} \quad \varphi \circ \varphi^{-1} = \mathrm{id}_B.$$

Proposición 2.3.5. *Sean $\varphi : R \longrightarrow S$ y $\psi : S \longrightarrow T$ dos homomorfismos de anillos.*

(1) La composición $\psi \circ \varphi : R \longrightarrow T$ es un homomorfismo de anillos.

(2) Si φ es un isomorfismo de anillos, entonces $\varphi^{-1} : S \longrightarrow R$ es un isomorfismo de anillos.

Demostración. La demostración de (1) es muy sencilla y la dejamos como ejercicio.
Demostramos (2). Sean $z_1, z_2 \in S$. Queremos ver que

$$\varphi^{-1}(z_1 + z_2) = \varphi^{-1}(z_1) + \varphi^{-1}(z_2). \tag{2.3.5.1}$$

Sean $x_1 = \varphi^{-1}(z_1)$ y $x_2 = \varphi^{-1}(z_2)$. Entonces (2.3.5.1) queda

$$\varphi^{-1}(z_1 + z_2) = x_1 + x_2$$

y esto equivale a

$$\varphi(x_1 + x_2) = z_1 + z_2. \tag{2.3.5.2}$$

Por la propiedad (1) de la definición 0.1.2 $\varphi(x_1 + x_2) = \varphi(x_1) + \varphi(x_2) = z_1 + z_2$, por lo que (2.3.5.2) es cierto.
La demostración de que

$$\varphi^{-1}(z_1 \cdot z_2) = \varphi^{-1}(z_1) \cdot \varphi^{-1}(z_2).$$

es análoga, usando en este caso la propiedad (2) de la definición 0.1.2.
La demostración de $\varphi^{-1}(1_S) = 1_R$ se sigue también de forma inmediata de la propiedad (3) de la definición 0.1.2 y la definición (2.3.4.1) de aplicación inversa. □

Observación 2.3.6. Sea $\varphi : R \longrightarrow S$ un isomorfismo de anillos. Aplicando la proposición 2.1.2 a φ y φ^{-1} concluimos que $\varphi(U(R)) = U(S)$. De igual forma, $x \in R$ es divisor de 0 en R si y solo si $\varphi(x)$ es divisor de 0 en S.

Ejemplos 2.3.7. Sean R y S anillos y sea R' un subanillo de R.

(1) La aplicación

$$\begin{array}{rccc} \mathrm{id}: & R & \longrightarrow & R \\ & x & \mapsto & x \end{array}$$

es un isomorfismo de anillos.

(2) La aplicación

$$\begin{array}{rccc} i: & R' & \longrightarrow & R \\ & x & \mapsto & x \end{array}$$

es un homomorfismo de anillos inyectivo.

(3) Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos. Consideramos la aplicación

$$\begin{array}{rccc} \varphi|_{R'}: & R' & \longrightarrow & S \\ & x' & \mapsto & \varphi(x') \end{array}$$

que se obtiene al restringir φ a R'. Como $\varphi|_{R'} = \varphi \circ i$, se sigue de la proposición 2.3.5, (1) que $\varphi|_{R'}$ es un homomofismo de anillos.

Ejemplo 2.3.8. La aplicación

$$\begin{array}{rccc} \varphi: & \mathbf{R}[X] & \longrightarrow & \mathbf{R}[X] \\ & f(X) & \mapsto & f'(X) \end{array}$$

no es un homomorfismo de anillos. Aunque se cumple la propiedad (i) de la definición 2.3.1, no se cumple (ii), ya que, en general, dados $f_1, f_2 \in \mathbf{R}[X]$, $(f_1 f_2)' = f_1' f_2 + f_1 f_2'$ no es igual a $f_1' f_2'$. Tampoco se cumple la propiedad (iii) de la definición 2.3.1, ya que la derivada del polinomio constante 1 es el polinomio constante 0.

Homomorfismos destacables:

Ejemplo 2.3.9. Sea R un dominio de integridad y sea K el cuerpo de fracciones de R. La manera en que se definieron las operaciones de K en la proposición-definición 1.4.4 implica que la aplicación

$$\begin{array}{rccc} i: & R & \longrightarrow & K \\ & x & \mapsto & x/1 \end{array}$$

es un homomorfismo de anillos. Además es inyectivo ya que si $x, y \in R$ son tales que $i(x) = i(y)$, entonces, por (1.4.4.2), $x/1 = y/1$ implica $x = y$.

Ejemplo 2.3.10. Sea R un anillo y sea I un ideal de R. La aplicación

$$\begin{array}{rccc} \pi: & R & \longrightarrow & R/I \\ & x & \mapsto & \overline{x} \end{array}$$

es un homomorfismo de anillos sobreyectivo.
Lo comprobamos a continuación. Dados $x, y \in R$, de (i) de la proposición 2.2.4 se sigue

$$\pi(x + y) = \overline{x + y} = \overline{x} + \overline{y} = \pi(x) + \pi(y).$$

Dados $x, y \in R$, de (ii) de la proposición 2.2.4 se sigue

$$\pi(xy) = \overline{xy} = \overline{x} \cdot \overline{y} = \pi(x)\pi(y).$$

Por último, $\pi(1) = \overline{1}$, que es el neutro del producto en R/I.
Como acabamos de ver las operaciones en el cociente R/I se definieron en la proposición 2.2.4 justo de manera que π fuera un homomorfismo de anillos.
El homomorfismo π es sobreyectivo, ya que un elemento cualquiera de R/I es de la forma $\overline{x}$ para algún $x \in R$, es decir, es de la forma $\pi(x)$ para algún $x \in R$.
A π se le denomina *proyección canónica* de R al anillo cociente R/I.

Ejercicio 2.3.11. Sea R un subanillo de un anillo S, sea $R[X]$ el anillo de polinomios en una variable con coeficientes en R y sea $z \in S$. Consideramos la aplicación

$$\begin{array}{rccc} \varphi: & R[X] & \longrightarrow & S \\ & f(X) & \mapsto & f(z), \end{array} \tag{2.3.11.1}$$

donde, si

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n,$$

con $a_0, a_1, \ldots, a_n \in R$, entonces

$$f(z) := a_0 + a_1z + a_2z^2 + \cdots + a_nz^n.$$

Demuestra que φ es un homomorfismo de anillos y que es sobreyectivo si $R = S$.
A φ se le denomina *homomorfismo de evaluación* (en z).

Observación 2.3.12. Sea R un subanillo de un anillo S, sea $R[X_1, \ldots, X_n]$ el anillo de polinomios en n variables con coeficientes en R y sean $z_1, \ldots, z_n \in S$. Usando induccíion en n podemos generalizar la definición del homomorfismo (2.3.11.1) al siguiente homomorfismo

$$\begin{array}{rccc} \varphi: & R[X_1, \ldots, X_n] & \longrightarrow & S \\ & f(X_1, \ldots, X_n) & \mapsto & f(z_1, \ldots, z_n), \end{array} \tag{2.3.12.1}$$

donde $f(z_1, \ldots, z_n)$ es el resultado de evaluar el polinomio $f(X_1, \ldots, X_n)$ de $R[X_1, \ldots, X_n]$ en la n–upla $(z_1, \ldots, z_n)$, es decir, el resultado de sustituir cada variable X_i por el elemento z_i de S. A φ se le denomina homomorfismo de evaluación en $z_1, \ldots, z_n$.

El núcleo y la imagen de un homomorfismo de anillos:

Proposición 2.3.13. *Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos, sea I un ideal de R y sea J un ideal de S.*

(1) $\varphi^{-1}(J)$ (que es la imagen inversa de J por el homomorfismo φ) es un ideal de R.

(2) Si φ es sobreyectivo, entonces $\varphi(I)$ es un ideal de S.

Demostración. (1) Recordemos que $\varphi^{-1}(J) = \{x \in R \mid \varphi(x) \in J\}$. Sean $x, y \in \varphi^{-1}(J)$ y sean $\lambda, \mu \in R$. Por la proposición 2.1.3, para ver que $\varphi^{-1}(J)$ es un ideal de R es suficiente ver que $\lambda x + \mu y \in \varphi^{-1}(J)$. Esto es equivalente a $\varphi(\lambda x + \mu y) \in J$. Esto es cierto ya que $\varphi(\lambda x + \mu y) = \varphi(\lambda x) + \varphi(\mu y) = \varphi(\lambda)\varphi(x) + \varphi(\mu)\varphi(y)$ está en J, pues $\varphi(x), \varphi(y) \in J$ y $\varphi(\lambda), \varphi(\mu) \in S$.

Recordemos que $\varphi(I) = \{\varphi(x) \mid x \in I\}$. Sean $z, w \in \varphi(I)$ y sean $\gamma, \delta \in S$. Por la proposición 2.1.3, para ver que $\varphi(I)$ es un ideal de S es suficiente ver que $\gamma z + \delta w \in \varphi(I)$. Como $z, w \in \varphi(I)$, existen $x, y \in I$ tales que $\varphi(x) = z, \varphi(y) = w$. Como φ es sobreyectivo, existen $\lambda, \mu \in R$ tales que $\varphi(\lambda) = \gamma$ y $\varphi(\mu) = \delta$. Entonces $\gamma z + \delta w = \varphi(\lambda)\varphi(x) + \varphi(\mu)\varphi(y) = \varphi(\lambda x) + \varphi(\mu y) = \varphi(\lambda x + \mu y)$, que pertenece a $\varphi(I)$, ya que, como $x, y \in I$ y $\lambda, \mu \in R$, $\lambda x + \mu y \in I$. □

Observación 2.3.14. Si $\varphi : R \longrightarrow S$ es un homomorfismo de anillos no sobreyectivo e I es un ideal de R, entonces $\varphi(I)$ no es en general un ideal. Por ejemplo, si φ es la inclusión de $\mathbf{Z}$ en $\mathbf{Q}$, n es un número natural e $I = (n)$, entonces $\varphi(I)$ no es un ideal de $\mathbf{Q}$, ya que, al ser $\mathbf{Q}$ un cuerpo, sus únicos ideales son (0) y (1) = $\mathbf{Q}$ (proposición 2.1.12). Más en general, si $\varphi : R \longrightarrow S$ es un homomorfismo de anillos no sobreyectivo, $\varphi((1_R))$ no es un ideal de S, ya que, si lo fuera, como $1_S = \varphi(1_R) \in \varphi((1_R))$, tendríamos $\varphi((1_R)) = S$, contradiciendo que φ no es sobreyectivo.

Definición 2.3.15. Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos. El *núcleo* de φ, denotado $\mathrm{Ker}\varphi$ es

$$\mathrm{Ker}\varphi = \{x \in R \mid \varphi(x) = 0_S\}.$$

Proposición 2.3.16. *Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos. El núcleo de φ es un ideal de R.*

Demostración. Como $\mathrm{Ker}\varphi = \varphi^{-1}((0_S))$ la proposición es una consecuencia inmediata de la proposición 2.3.13. De todas formas damos a continuación una demostración independiente.

Sean $x, y \in \mathrm{Ker}\varphi$ y $\lambda, \mu \in R$. Por la proposición 2.1.3 bastaría ver $\lambda x + \mu y \in \mathrm{Ker}\varphi$. De (i) y (ii) de la definición 2.3.1 se sigue de

$$\varphi(\lambda x + \mu y) = \varphi(\lambda x) + \varphi(\mu y) = \varphi(\lambda)\varphi(x) + \varphi(\mu)\varphi(y),$$

que es 0, ya que $\varphi(x) = \varphi(y) = 0$ porque $x, y \in \mathrm{Ker}\varphi$. Como $\varphi(\lambda x + \mu y) = 0$, tenemos que $\lambda x + \mu y \in \mathrm{Ker}\varphi$ como queríamos. □

Ejemplo 2.3.17. Sea R un anillo, sea I un ideal de R y sea π la proyección canónica de R a R/I. El núcleo de π es I. En efecto, $x \in \mathrm{Ker}\pi$ si y solo si $\pi(x) = 0$, es decir, si y solo si $\overline{x} = \overline{0}$. Esto equivale a $x \sim_I 0$, es decir, a que $x \in I$.

Proposición 2.3.18. *Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos. Entonces φ es inyectivo si y solo si $\mathrm{Ker}\varphi = (0_R)$.*

Demostración. Veamos primero que si φ es inyectivo, entonces $\mathrm{Ker}\varphi = (0_R)$. Como $\mathrm{Ker}\varphi$ es un ideal, $0_R \in \mathrm{Ker}\varphi$, por lo que basta ver que $\mathrm{Ker}\varphi \subset (0_R)$. Sea $x \in \mathrm{Ker}\varphi$. Entonces $\varphi(x) = 0_S$. Como $0_R \in \mathrm{Ker}\varphi$, $\varphi(0_R) = 0_S$. Como φ es inyectivo, $\varphi(x) = 0_S = \varphi(0_R)$ implica $x = 0_R$.

Veamos ahora que si $\mathrm{Ker}\varphi = (0_R)$, entonces φ es inyectivo. Sean $x, y \in R$ tales que $\varphi(x) = \varphi(y)$. Entonces $\varphi(x - y) = \varphi(x) + \varphi(-y) = \varphi(x) - \varphi(y) = 0_S$, de donde $x - y \in \mathrm{Ker}\varphi$. Como $\mathrm{Ker}\varphi = (0_R)$, se sigue que $x - y = 0_R$, es decir, $x = y$. □

Profundizamos a continuación en el ejemplo 2.3.9:

Ejercicio 2.3.19. Sea R un dominio de integridad y sea K el cuerpo de fracciones de R. Sea K' un cuerpo y sea $i' : R \longrightarrow K'$ un homomorfismo de anillos inyectivo. Entonces existe un único homomorfismo de anillos $j : K \longrightarrow K'$ (necesariamente inyectivo; véase el ejercicio 5 de la hoja 2) tal que el siguiente diagrama es *conmutativo*

$$\begin{array}{ccc} R & \xrightarrow{i'} & K' \\ {\scriptstyle i}\downarrow & \nearrow_{j} & \\ K & & \end{array},$$

es decir, $i' = j \circ i$.

Indicación: define $j(x/y)$ como $i'(x)(i'(y))^{-1}$ (¿por qué $i'(y) \neq 0$?).

Observación 2.3.20. En la observación 1.4.5 vimos de manera intuitiva que el cuerpo de fracciones de R es el cuerpo "más pequeño" que contiene a R. El ejercicio 2.3.19 nos permite justificar esto de manera más rigurosa. Si identificamos R con los subanillos $i(R)$ en K e $i'(R)$ en K' y K con el subanillo $j(K)$ de K', entonces K es el cuerpo "más pequeño" que contiene a R, puesto que si R es un subanillo de un cuerpo K', entonces K es un subanillo de K'.

Proposición 2.3.21. *Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos. La imagen de φ es un subanillo de S.*

Demostración. Sean $z, w \in \mathrm{im}\varphi$. Entonces existen $x, y \in R$ tales que $\varphi(x) = z, \varphi(y) = w$. Entonces $z - w = \varphi(x) - \varphi(y) = \varphi(x - y) \in \mathrm{im}\varphi$. Asimismo $zw = \varphi(x)\varphi(y) = \varphi(xy) \in \mathrm{im}\varphi$. Finalmente, como $\varphi(1_R) = 1_S$ tenemos que $1_S \in \mathrm{im}\varphi$. □

Corolario 2.3.22. *Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos y sea R' un subanillo de R. Entonces $\varphi(R')$ es un subanillo de S.*

Demostración. Consideramos el homomorfismo $\varphi|_{R'} : R' \longrightarrow S$ que se obtiene al restringir φ a R' (véase el ejemplo 2.3.7, (3)). Como $\varphi(R') = \mathrm{im}(\varphi|_{R'})$, el resultado se sigue de la proposición 2.3.21. □

Ejemplo 2.3.23. Sea R un subanillo de un anillo S, sea $R[X_1, \ldots, X_n]$ el anillo de polinomios en n variables con coeficientes en R y sean $z_1, \ldots, z_n \in S$. La imagen del homomorfismo (2.3.12.1) de evalaución en $z_1, \ldots, z_n$ es un subanillo de S, que denominamos *subanillo generado por R y por $z_1, \ldots, z_n$* y denotamos por $R[z_1, \ldots, z_n]$.
El subanillo $R[z_1, \ldots, z_n]$ consiste en "expresiones polinómicas" en $z_1, \ldots, z_n$ con coeficientes en R, es decir, en sumas finitas de elementos de S de la forma

$$a_{m_1,m_2,\ldots,m_n} z_1^{m_1} z_2^{m_2} \cdots z_n^{m_n},$$

donde $m_1, m_2, \ldots, m_n \in \mathbf{N}$ y $a_{m_1,m_2,\ldots,m_n} \in R$. Por ejemplo, dado $z \in S$,

$$R[z] = \{a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m \mid m \in \mathbf{N} \cup \{0\}, a_0, a_1, \ldots, a_n \in R\}. \tag{2.3.23.1}$$

Ilustramos el ejemplo 2.3.23 en los siguientes casos más concretos:

Ejemplos 2.3.24. Sea d un número entero que no es un cuadrado (es decir, tal que no existe $c \in \mathbf{Z}$ que cumple $d = c^2$). Sea $\sqrt{d}$ una de las dos raíces cuadradas de d en $\mathbf{C}$.

(1) El subanillo $\mathbf{Z}[\sqrt{d}]$ de $\mathbf{C}$ es

$$\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbf{Z}\}.$$

En efecto, por (2.3.23.1)

$$\mathbf{Z}[\sqrt{d}] = \{a_0 + a_1\sqrt{d} + a_2(\sqrt{d})^2 + \cdots + a_m(\sqrt{d})^m \mid m \in \mathbf{N} \cup \{0\}, a_0, a_1, \ldots, a_n \in \mathbf{Z}\}.$$

Como $(\sqrt{d})^2 = d, (\sqrt{d})^3 = d\sqrt{d}, (\sqrt{d})^4 = d^2$, etc., toda expresión de la forma $a_0 + a_1\sqrt{d} + a_2(\sqrt{d})^2 + \cdots + a_m(\sqrt{d})^m$ se puede escribir $a + b\sqrt{d}$ (con $a = a_0 + a_2 d + a_4 d^2 + \cdots$ y $b = a_1 + a_3 d + a_5 d^2 + \cdots$).

(2) De igual forma el subanillo $\mathbf{Q}[\sqrt{d}]$ de $\mathbf{C}$ es

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

Ideales del anillo cociente:

Pasamos ahora a describir cómo son los ideales de un anillo cociente R/I, relacionándolos con ideales de R:

Teorema 2.3.25. *(de correspondencia). Sea R un anillo, sea I un ideal de R y sea $\pi : R \longrightarrow R/I$ el homomorfismo de proyección canónica definido en el ejemplo 2.3.10. La aplicación*

$$\begin{array}{ccc} \{I' \text{ ideal de } R \mid I \subset I'\} & \longrightarrow & \{\text{ideales de } R/I\} \\ I' & \mapsto & \pi(I') \end{array} \tag{2.3.25.1}$$

es una correspondencia biyectiva entre el conjunto $\{I'$ ideal de $R \mid I \subset I'\}$ y el conjunto $\{$ideales de $R/I\}$. Su inversa es

$$\begin{array}{ccc} \{\text{ideales de } R/I\} & \longrightarrow & \{I' \text{ ideal de } R \mid I \subset I'\} \\ J & \mapsto & \pi^{-1}(J) \end{array} \tag{2.3.25.2}$$

En particular todo ideal J de R/I es la imagen directa de un ideal de R, ya que $J = \pi(\pi^{-1}(J))$. Además, si I'' es un ideal de R, entonces $\pi^{-1}(\pi(I'')) = I + I''$.

Demostración. Vemos primero que, si I'' es un ideal de R, entonces $\pi^{-1}(\pi(I'')) = I + I''$. En efecto, $x \in \pi^{-1}(\pi(I''))$ si y solo si $\pi(x) \in \pi(I'')$, es decir, si y solo si existe $y \in I''$ tal que $\pi(x) = \pi(y)$. Esto equivale a que $\pi(x - y) = 0$, que es lo mismo que $\overline{x - y} = \overline{0}$, que es lo mismo que $x - y \in I$. Esto equivale a que exista $z \in I$ tal que $x - y = z$, es decir, tal que $x = y + z$. Así pues hemos visto que $x \in \pi^{-1}(\pi(I''))$ equivale a que existan $y \in I$ y $z \in I''$ tales que $x = y + z$. Esto prueba $\pi^{-1}(\pi(I'')) = I + I''$.

Veamos ahora que la aplicación de (2.3.25.1) va al conjunto de ideales de R/I. Como π es un homomorfismo sobreyectivo, entonces por la proposición 2.3.13 (2), para todo ideal I' de R se tiene que $\pi(I')$ es un ideal de R/I.

Veamos ahora que la aplicación de (2.3.25.2) va al conjunto de ideales de R que contienen a I. Sea J un ideal de R/I. Por la proposición 2.3.13 (1) tenemos que $\pi^{-1}(J)$ es un ideal de R. Por otra parte $\overline{0} \in J$, por lo que $\pi^{-1}(0) \subset \pi^{-1}(J)$. Como $\pi^{-1}(0)$ es el núcleo de π y, según el ejemplo 2.3.17, el núcleo de π es I, tenemos que $I \subset \pi^{-1}(J)$.

Finalmente vemos cuál es la composición de las aplicaciones de (2.3.25.1) y (2.3.25.2) en uno y otro sentido. Ya vimos que si I' es un ideal de R, entonces $\pi^{-1}(\pi(I')) = I + I'$. Si además $I \subset I'$, entonces $\pi^{-1}(\pi(I')) = I + I' = I'$, por que la composición de la aplicación (2.3.25.1) seguida de la aplicación (2.3.25.2) es la identidad.

Por otra parte, si J es un ideal de R/I, como π es una aplicación sobreyectiva, $\pi(\pi^{-1}(J)) = J$, por lo que la composición de la aplicación (2.3.25.2) seguida de la aplicación (2.3.25.1) es la identidad. □

Notación 2.3.26. Sea R un anillo y sea I un ideal de R. Sea I' un ideal de R tal que $I \subset I'$. El ideal $\pi(I')$ de R/I se denota I'/I.

2.4 El teorema de isomorfía

Ya hemos visto que, en general, un homomorfismo de anillos no tiene por qué ser ni inyectivo ni sobreyectivo. En esta sección vamos a ver cómo, a partir de un homomorfismo cualquiera, podemos obtener un isomorfismo. La idea es la siguiente. Dado $\varphi : R \longrightarrow S$ un homomorfismo de anillos, para hacer que sea sobreyectivo consideramos como su anillo de llegada la imagen de φ, que es un subanillo S' de S, es decir, consideramos el homomofismo

$$\begin{array}{rccc} \psi: & R & \longrightarrow & S' \\ & x & \mapsto & \varphi(x), \end{array}$$

que es siempre sobreyectivo pues, por construcción, la imagen de ψ es igual a la imagen de φ, que es S'. Para modificar ψ hasta conseguir un homomofismo inyectivo hacemos lo siguiente. Recordemos que, según la proposición 2.3.18, un homomofismo es inyectivo si y solo si su núcleo es nulo. Entonces, el obstáculo para que ψ sea inyectivo sería que existieran elementos no nulos en el núcleo de ψ. Así, lo que vamos a hacer es "matar" esos elementos no nulos del núcleo de ψ. Para ello, definiremos, a partir de ψ, un homomorfismo ψ' que parta del cociente $R/\mathrm{Ker}\psi$. Hacer cociente por un ideal I de R tiene el efecto de "matar" los elementos de I. Dicho de forma más precisa, la clase $\overline{y}$ de un elemento y de I es $\overline{0}$. Como los elementos de $\mathrm{Ker}\psi$ son aquellos $x \in R$ tales que $\psi(x) = 0$, la idea es que, como sus clases $\overline{x}$ en $R/\mathrm{Ker}\psi$ serán todas $\overline{0}$, el único elemento de $R/\mathrm{Ker}\psi$ cuya imagen por ψ' es nula será $\overline{0}$, es decir, el núcleo de ψ' será trivial o, lo que es lo mismo, ψ' será inyectivo. Por supuesto, estas ideas intuitivas requieren ser formalizadas y hay varias comprobaciones a realizar. Así lo haremos en el enunciado y la demostración del teorema 2.4.1. Es posible que estas ideas y este teorema te resulte familiar si en Álgebra Lineal viste el teorema análogo para aplicaciones lineales entre espacios vectoriales.

Teorema 2.4.1. *(de isomorfía). Dado un homomofismo de anillos $\varphi : R \longrightarrow S$ se tiene el diagrama*

(2.4.1.1)
$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ \dfrac{R}{\mathrm{Ker}\varphi} & \xrightarrow{\overline{\varphi}} & \mathrm{im}\varphi, \end{array}$$

que es conmutativo, *es decir, $\varphi = i \circ \overline{\varphi} \circ \pi$. En el diagrama* (2.4.1.1)*, la aplicación π es la proyección canónica de R al cociente $R/\mathrm{Ker}\varphi$, la aplicación i es la inclusión de* $\mathrm{im}\varphi$ *en S y $\overline{\varphi}$ viene definida por*

$$\begin{array}{rccc} \overline{\varphi}: & R/\mathrm{Ker}\varphi & \longrightarrow & \mathrm{im}\varphi \\ & \overline{x} & \mapsto & \varphi(x). \end{array}$$

La aplicación $\overline{\varphi}$ está bien definida y es un isomorfismo de anillos.

Demostración. (i) Para que el diagrama (2.4.1.1) tenga sentido tenemos que comprobar que $\overline{\varphi}$ está bien definida, es decir, que es realmemte una aplicación de $R/\mathrm{Ker}\varphi$ a $\mathrm{im}\varphi$. Como $\overline{\varphi}$ se define usando representantes, para ello debemos ver que, dado $\overline{x} \in R/\mathrm{Ker}\varphi$, la imagen de $\overline{x}$ por $\overline{\varphi}$ no depende del representante de $\overline{x}$ elegido. Sea pues $x' \in R$ tal que $\overline{x} = \overline{x'}$. Esto quiere decir que $x - x' \in \mathrm{Ker}\varphi$, es decir, que $\varphi(x - x') = 0$. Como φ es un homomofismo, $\varphi(x-x') = \varphi(x)-\varphi(x')$, por lo que $\varphi(x)-\varphi(x') = 0$ y $\varphi(x) = \varphi(x')$. Entonces, si definimos la imagen de $\overline{x}$ por $\overline{\varphi}$ usando el representante x, tenemos $\overline{\varphi}(\overline{x}) = \varphi(x)$ y si definimos la imagen de $\overline{x}$ por $\overline{\varphi}$ usando el representante x', tenemos $\overline{\varphi}(\overline{x'}) = \varphi(x')$. Como hemos visto que $\varphi(x) = \varphi(x')$, ambas imágenes coinciden. Por otra parte es claro que $\overline{\varphi}$ termina en el anillo $\mathrm{im}\varphi$, ya que, para todo $x \in R$, $\overline{\varphi}(\overline{x}) = \varphi(x)$, que pertenece a $\mathrm{im}\varphi$.

(ii) Vemos ahora que $\varphi = i \circ \overline{\varphi} \circ \pi$. Para todo $x \in R$, $\pi(x) = \overline{x}$ y para todo $y \in \mathrm{im}\varphi$, $i(y) = y$. Como $\overline{\varphi}(\overline{x}) = \varphi(x)$, entonces para todo $x \in R$,

$$(i \circ \overline{\varphi} \circ \pi)(x) = (i \circ \overline{\varphi})(\pi(x)) = (i \circ \overline{\varphi})(\overline{x}) = i(\overline{\varphi}(\overline{x})) = i(\varphi(x)) = \varphi(x),$$

es decir, para cada $x \in R$, la aplicación φ y la aplicación $i \circ \overline{\varphi} \circ \pi$ toman el mismo valor.

(iii) Vemos ahora que $\overline{\varphi}$ es un homomorfismo de anillos. Para ello debemos comprobar que, para cualesquiera $x, y \in R$ y sus clases $\overline{x}, \overline{y}$ en $R/\mathrm{Ker}\varphi$, tenemos que comprobar que

$$\begin{gathered}\overline{\varphi}(\overline{x} + \overline{y}) = \overline{\varphi}(\overline{x}) + \overline{\varphi}(\overline{y}) \\ \overline{\varphi}(\overline{x} \cdot \overline{y}) = \overline{\varphi}(\overline{x}) \cdot \overline{\varphi}(\overline{y}) \\ \overline{\varphi}(\overline{1}_R) = 1_S,\end{gathered}$$

que es también el elemento neutro del producto en $\mathrm{im}\varphi$. De la definición de suma y producto en el cociente, de la definición de $\overline{\varphi}$ y del hecho de que φ sea un homomorfismo de anillos, se deduce

$$\overline{\varphi}(\overline{x} + \overline{y}) = \overline{\varphi}(\overline{x + y}) = \varphi(x + y) = \varphi(x) + \varphi(y) = \overline{\varphi}(\overline{x}) + \overline{\varphi}(\overline{y}),$$

$$\overline{\varphi}(\overline{x} \cdot \overline{y}) = \overline{\varphi}(\overline{x \cdot y}) = \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = \overline{\varphi}(\overline{x}) \cdot \overline{\varphi}(\overline{y})$$

y

$$\overline{\varphi}(\overline{1}_R) = \varphi(1_R) = 1_S.$$

(iv) Vemos ahora que $\overline{\varphi}$ es inyectivo. Para ello comprobamos que el núcleo de $\overline{\varphi}$ es nulo. En efecto, dado $\overline{x} \in R/\mathrm{Ker}\varphi$, la clase $\overline{x}$ pertenece al núcleo de $\overline{\varphi}$ si y solo si $\overline{\varphi}(\overline{x}) = 0_S$. Por la definición de $\overline{\varphi}$ esto es equivalente a que $\varphi(x) = 0_S$ y esto a que x pertenezca al núcleo de φ. Esto último equivale a que la clase $\overline{x}$ de x en el cociente $R/\mathrm{Ker}\varphi$ sea $\overline{0}_R$. Así pues, el único elemento en el núcleo de $\overline{\varphi}$ es $\overline{0}_R$.

(v) Para finalizar la demostración comprobamos que $\overline{\varphi}$ es sobreyectivo. Sea $y \in \mathrm{im}\varphi$. Entonces existe $x \in R$ tal que $y = \varphi(x)$. Por la definición de $\overline{\varphi}$, la clase $\overline{x}$ de x cumple $\overline{\varphi}(\overline{x}) = \varphi(x) = y$. □

Observación 2.4.2. Sea $\varphi : R \longrightarrow S$ un homomofismo de anillos y sea I un ideal de R contenido en el núcleo de φ. Argumentando como en (i) y (iii) de la demostración del teorema 2.4.1 podemos construir una aplicación bien definida

$$\begin{array}{rccc} \widetilde{\varphi}: & R/I & \longrightarrow & S \\ & \overline{x} & \mapsto & \varphi(x) \end{array}$$

que es un homomorfismo de anillos. La diferencia entre $\widetilde{\varphi}$ y el homomorfismo $\overline{\varphi}$ del teorema 2.4.1 es que $\widetilde{\varphi}$ no será en general un isomorfismo (será inyectivo si y solo si $I = \text{Ker}\varphi$, sobreyectivo si y solo si $\text{im}\varphi = S$ y si ocurren ambas cosas, $\widetilde{\varphi} = \overline{\varphi}$); aun así hay situaciones en que será útil construir un homomorfismo como $\widetilde{\varphi}$.

El teorema 2.4.1 es uno de los resultados más importantes del curso y lo usaremos en muchas aplicaciones y ejercicios. Vemos ahora algunas.

Ejemplo 2.4.3. Sea R un anillo y sea $R[X]$ el anillo de polinomios en una variable con coeficientes en R. Los anillos $R[X]/(X)$ y R son isomorfos.

Para verlo usamos el teorema 2.4.1. La clave es escoger el homorfismo de $R[X]$ a R adecuado que juegue el papel de φ en el teorema 2.4.1. En este caso consideramos el homomorfismo de evaluación (véase el ejercicio 2.3.11)

$$\begin{array}{rccc} \varphi: & R[X] & \longrightarrow & R \\ & f(X) & \mapsto & f(0) \end{array}$$

en $0 \in R$.

El homomofismo φ es sobreyectivo ya que, dado $a \in R$, la evaluación del polinomio constante a en 0 es a.

Veamos ahora que el núcleo de φ es el ideal (X) generado por X. Sea

$$f(X) = a_0 + a_1X + \cdots + a_nX_n \in R[X],$$

donde n es un entero no negativo y $a_0, a_1, \ldots, a_n \in R$. Entonces $f \in \text{Ker}\varphi$ si y solo si $\varphi(f) = 0$. Esto equivale a $0 = f(0) = a_0$. Esta última condición es equivalente a que f sea múltiplo de X, es decir, a que $f \in (X)$.

Aplicamos finalmente el teorema 2.4.1. Como φ es sobreyectiva, $\text{im}\varphi = R$ y como $\text{Ker}\varphi = (X)$, $\overline{\varphi}$ es un isomorfismo entre $R[X]/(X)$ y R. El isomorfismo $\overline{\varphi}$ identifica la clase $\overline{f}$ en $R[X]/(X)$ de un polinomio $f(X)$ de $R[X]$ con el valor que $f(X)$ toma en 0.

Ejemplo 2.4.4. El ejemplo 2.4.3 se puede generalizar así. Sea R un anillo y sea $a \in R$. Los anillos $R[X]/(X - a)$ y R son isomorfos. Para comprobar esto consideramos el homomorfismo

$$\begin{array}{rccc} \varphi_a: & R[X] & \longrightarrow & R \\ & f(X) & \mapsto & f(a) \end{array}$$

de evaluación en a (véase el ejercicio 2.3.11). El homomorfismo φ_a es la composición $\varphi_a = \varphi_0 \circ t_a$, donde φ_0 es el homomofismo φ del ejemplo 2.4.3, es decir, el homomofismo de evaluación en 0 y t_a es

$$\begin{array}{rccc} t_a: & R[X] & \longrightarrow & R[X] \\ & f(X) & \mapsto & f(X+a) \end{array}$$

es también un homomorfismo de evaluación, de hecho, un isomorfismo, ya que tiene inverso, que es

$$\begin{array}{rccc} t_{-a}: & R[X] & \longrightarrow & R[X] \\ & f(X) & \mapsto & f(X-a). \end{array}$$

Como φ_0 es sobreyectivo y t_a es biyectivo, φ_a es sobreyectivo. Por otra parte

$$\mathrm{Ker}\varphi_a = \varphi_a^{-1}(0) = t_a^{-1}(\varphi_0^{-1}(0)) = t_{-a}(\mathrm{Ker}\varphi_0) = t_{-a}((X)) = (X-a)$$

(recordemos que, según vimos en el ejemplo 2.4.3, $\mathrm{Ker}\varphi_0 = (X)$). Aplicando el teorema 2.4.1 a φ_a concluimos que $\overline{\varphi_a}$ es un isomorfismo entre $R[X]/(X-a)$ y R. El isomorfismo $\overline{\varphi_a}$ identifica la clase $\overline{f}$ de un polinomio f de $R[X]$ con el valor de R que toma f en a. Por tanto, dos polinomios f_1 y f_2 de $R[X]$ tienen la misma clase $\overline{f_1} = \overline{f_2}$ en $R[X]/(X-a)$ si y solo si $f_1(a) = f_2(a)$ (compara con el ejercicio 2.2.9).

Ejemplo 2.4.5. El ejemplo 2.4.3 se puede generalizar a varias variables. Sea R un anillo y sea $R[X_1, \ldots, X_n]$ el anillo de polinomios en n variables con coeficientes en R. Los anillos $R[X_1, \ldots, X_n]/(X_1, \ldots, X_n)$ y R son isomorfos. Para evitar una complicación excesiva en la notación haremos el argumento para dos variables X, Y, siendo similar el argumento en el caso general. En este caso consideramos el homomorfismo de evaluación en $(0,0)$

$$\begin{array}{rccc} \varphi: & R[X,Y] & \longrightarrow & R \\ & f(X,Y) & \mapsto & f(0,0), \end{array}$$

definido en (2.3.12.1). Aplicaremos a φ el teorema 2.4.1.

Por las mismas razones usadas en el ejemplo 2.4.3, φ es sobreyectivo. Veamos ahora que el núcleo de φ es el ideal (X, Y) generado por X e Y. En efecto, f pertenece al núcleo de φ si y solo si $f(0,0) = 0$ y esto equivale a que $f(X, Y)$ tenga término independientes nulo. Esto es equivalente a que existan $f_1, f_2 \in R[X, Y]$ tales que $f = f_1 \cdot X + f_2 \cdot Y$, es decir, a que $f \in (X, Y)$.

Aplicamos finalmente el teorema 2.4.1. Como φ es sobreyectiva, $\mathrm{im}\varphi = R$ y como $\mathrm{Ker}\varphi = (X, Y)$, $\overline{\varphi}$ es un isomorfismo entre $R[X, Y]/(X, Y)$ y R. El isomorfismo $\overline{\varphi}$ identifica la clase $\overline{f}$ en $R[X, Y]/(X, Y)$ de un polinomio $f(X, Y)$ de $R[X, Y]$ con el valor que $f(X, Y)$ toma en $(0, 0)$. Por tanto, dos polinomios f_1 y f_2 de $R[X, Y]$ tienen la misma clase $\overline{f_1} = \overline{f_2}$ en $R[X, Y]/(X, Y)$ si y solo si $f_1(0, 0) = f_2(0, 0)$.

Ejemplo 2.4.6. Los anillos $\mathbf{R}[X]/(X^2 + 1)$ y $\mathbf{C}$ son isomorfos.

Para verlo aplicaremos el teorema 2.4.1 al homomorfismo de evaluación (véase el ejercicio 2.3.11)

$$\begin{array}{rccc} \varphi: & \mathbf{R}[X] & \longrightarrow & \mathbf{C} \\ & f(X) & \mapsto & f(i) \end{array}$$

en $i \in \mathbf{C}$.

El homomofismo φ es sobreyectivo ya que, dado un elemento cualquiera $a + bi$ de $\mathbf{C}$ ($a, b \in \mathbf{R}$) se tiene que $\varphi(a + bX) = a + bi$.

Veamos ahora que el núcleo de φ es el ideal (X^2+1) de $\mathbf{R}[X]$, generado por X^2+1. Vemos primero que $(X^2 + 1)$ está contenido en el núcleo de φ. La imagen de $X^2 + 1$ por φ es $i^2 + 1 = 0$, por lo que $X^2 + 1$ pertenece al núcleo de φ. Como el núcleo de φ es un ideal de $\mathbf{R}[X]$, todos los múltiplos de $X^2 + 1$ están en el núcleo de φ, es decir, $(X^2 + 1)$ está contenido en el núcleo de φ.

Vemos ahora que el núcleo de φ está contenido en $(X^2 + 1)$. Dado $f(X) \in \mathbf{R}[X]$, lo dividimos entre $X^2 + 1$ utilizando el algoritmo de división de polinomios usual.[4] Así existe un polinomio $q(X)$ de $\mathbf{R}[X]$ y elementos a_0, a_1 de $\mathbf{R}$ tales que

$$f(X) = (X^2 + 1) \cdot q(X) + a_1X + a_0, \tag{2.4.6.1}$$

ya que el resto de dividir $f(X)$ por X^2+1, que es un polinomio de grado 2, es un polinomio de grado menor que 2. Si $f(X)$ pertenece al núcleo de φ, entonces $0 = \varphi(f) = a_0 + a_1i$, ya que $\varphi(X^2 + 1) = 0$ como ya hemos observado. Un número complejo $a_0 + a_1i$ es 0 si y solo si $a_0 = a_1 = 0$, así que (2.4.6.1) queda $f(X) = q(X) \cdot (X^2 + 1)$, es decir, f pertenece al ideal generado por $X^2 + 1$, de donde el núcleo de φ está contenido en $(X^2 + 1)$.

Aplicamos finalmente el teorema 2.4.1. Como φ es sobreyectivo, $\mathrm{im}\varphi = \mathbf{C}$ y como $\mathrm{Ker}\varphi = (X^2 + 1)$, $\overline{\varphi}$ es un isomorfismo entre $\mathbf{R}[X]/(X^2 + 1)$ y $\mathbf{C}$.

Ejemplo 2.4.7. Los anillos $\mathbf{Z}[X]/(2, X)$ y $\mathbf{Z}/(2)$ son isomorfos. Para ello consideramos la aplicación

$$\begin{array}{rccc} \varphi: & \mathbf{Z}[X] & \longrightarrow & \mathbf{Z}/(2) \\ & f(X) & \mapsto & \overline{f(0)}, \end{array}$$

donde $f(0)$ es la evaluación de $f(X)$ en 0 (que es número entero) y $\overline{f(0)}$ es la clase de $f(0)$ en $\mathbf{Z}/(2)$. Como la aplicación φ es la composición del homomofismo evaluación en 0 seguido de la proyección canónica de $\mathbf{Z}$ a $\mathbf{Z}/(2)$, la aplicación φ es un homomorfismo. Como tanto el homomofismo evaluación en 0 como la proyección canónica de $\mathbf{Z}$ a $\mathbf{Z}/(2)$ son sobreyectivos, φ también lo es.

El núcleo de φ es $(2, X)$ ya que un polinomio

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

[4] Suponemos que estás suficientemente familiariazado con este algoritmo. De todas formas lo repasaremos con detalle en la sección 3.1.

de $\mathbf{Z}[X]$ pertenece al núcleo de φ si y solo si $\overline{a_0} = \overline{0}$ en $\mathbf{Z}/(2)$, es decir, si y solo si a_0 es par. Esto es equivalente a que exista $b_0 \in \mathbf{Z}$ tal que

$$f(X) = 2b_0 + a_1X + \cdots + a_nX^n = b_0 \cdot 2 + (a_1 + a_2X \cdots + a_nX^{n-1}) \cdot X,$$

es decir, a que f pertenezca a $(2, X)$.
Aplicando el teorema 2.4.1 a φ obtenemos el resultado.

Este argumento se puede generalizar para demostrar que, dado $n \in \mathbf{N}$, los anillos $\dfrac{\mathbf{Z}[X]}{(n, X)}$ y $\mathbf{Z}/(n)$ son isomorfos. Otra forma de demostrarlo es usando el teorema 2.4.10.

El teorema 2.4.1 se suele llamar *primer teorema de isomorfía* porque de él se deducen otros dos. Antes de enunciar el primero de ellos necesitamos un resultado previo.

Proposición 2.4.8. *Sea R un anillo, sea S un subanillo de R y sea I un ideal de R. Definimos $S + I := \{a + y \mid a \in S, y \in I\}$. Entonces*

(1) $S + I$ es un subanillo de R;

(2) I es un ideal de $S + I$; y

(3) $S \cap I$ es un ideal de S.

Demostración. Sean $a_1, a_2 \in S$ e $y_1, y_2 \in I$. Entonces

$$(a_1 + y_1) - (a_2 + y_2) = (a_1 - a_2) + (y_1 - y_2) \in S + I,$$

ya que $a_1 - a_2 \in S$ por ser S un subanillo de R e $y_1 - y_2 \in I$ por ser I un ideal de R. Por otra parte

$$(a_1 + y_1)(a_2 + y_2) = a_1a_2 + a_1y_2 + a_2y_1 + y_1y_2 \in S + I,$$

ya que $a_1a_2 \in S$ por ser S un subanillo de R y $a_1a_2 + a_1y_2 + a_2y_1 + y_1y_2 \in I$ por ser I un ideal de R. Finalmente, $1 \in S$ porque S es un subanillo de R y $0 \in I$ porque I es un ideal de R, por lo que $1 = 1 + 0 \in S + I$. Con esto terminamos la demostración de (1).
La afirmación (2) se sigue del hecho, inmediato, de que un ideal de un anillo lo es también de un subanillo en el que esté contenido.
Por último, si i es el homomorfismo inclusión de S en R, entonces $S \cap I = i^{-1}(I)$. La afirmación (3) se sigue por tanto de la proposición 2.3.13. □

Teorema 2.4.9. *(segundo teorema de isomorfía). Sean R, S e I como en el enunciado de la proposición 2.4.8. Los anillos $S/(I \cap S)$ y $(S + I)/I$ son isomorfos.*

Demostración. Consideramos el homomofismo φ de S a $(S + I)/I$ que se obtiene componiendo la inclusión de S en $S + I$ seguida de la proyección canónica de $S + I$ a $(S + I)/I$.
El homomorfismo φ es sobreyectivo ya que, si $a \in S$ e $y \in I$, la clase, $\overline{a + y}$ en $(S + I)/I$ es igual a la clase $\overline{a}$, ya que $y \in I$. Por tanto, para todo $\overline{a + y}$ en $(S + I)/I$, $\varphi(a) = \overline{a} = \overline{a + y}$.

Por otra parte, los elementos a de S tales que $\varphi(a) = 0$ son aquellos cuya clase $\overline{a}$ en $(S+I)/I$ es $\overline{0}$, es decir, son aquellos elementos de S que están en I, es decir, los elementos de $S \cap I$. Así pues el núcleo de φ es $S \cap I$.

Aplicando el teorema 2.4.1 a φ, obtenemos el isomorfismo deseado. □

Teorema 2.4.10. *(tercer teorema de isomorfía). Sea R un anillo y sean $I \subset J$ dos ideales de R. Los anillos $R/I/(J/I)$ y R/J son isomorfos (por I/J nos referimos, según la notación 2.3.26 al ideal $\pi(J)$ de R/I, donde π es la proyección canónica de R a R/I).*

Demostración. Damos las ideas de la demostración dejando los detalles como ejercicio. Consideramos la aplicación

$$\begin{array}{rccc} \varphi: & R/I & \longrightarrow & R/J \\ & x+I & \mapsto & x+J \end{array}$$

(adoptamos en este caso la notación $x + I$ y $x + J$ para denotar clases de equivalencia en lugar de la notación $\overline{x}$ para evitar confusiones). La aplicación φ está bien definida porque $I \subset J$.

La aplicación φ es un homorfismo de anillos porque las operaciones en R/I y R/J se definen, en ambos casos, mediante la suma y producto en R de representantes y porque el neutro del producto en R/I es $1 + I$ y el neutro del producto en R/J es $1 + J$.

Dado un elemento $x + J$ en R/J, se tiene $\varphi(x + I) = x + J$, por lo que φ es sobreyectivo.

Dado $x + I \in R/I$, $\varphi(x + I) = 0 + J$ si y solo si $x \in J$. Esto quiere decir que $x + I \in J/I$, por lo que el núcleo de φ es J/I. El teorema se obtiene pues de aplicar el teorema 2.4.1 a φ. □

2.5 Ideales primos e ideales maximales

En esta sección estudiamos dos clases distinguidas de ideales, los ideales *primos* y los ideales *maximales*. Para motivar la noción de ideal primo comenzamos con un ejemplo:

Ejemplo 2.5.1. Sea p un número natural primo y sea $I = (p)$ el ideal generado por p en $\mathbf{Z}$. El ideal I posee la siguiente propiedad: dados $m_1, m_2 \in \mathbf{Z}$ tales que $m_1 m_2 \in I$, o bien $m_1 \in I$ o bien $m_2 \in I$. En efecto, si $m_1 m_2 \in I$, entonces existe $\lambda \in \mathbf{Z}$ tal que $m_1 m_2 = \lambda p$. Como p es primo, p aparece en la descomposición de $m_1 m_2$ como producto de primos; como podemos obtener esta descomposición multiplicando las descomposiciones de m_1 y de m_2, p aparece en una de las dos descomposiciones, de donde p divide a m_1 o a m_2, es decir, $m_1 \in I$ o $m_2 \in I$. [5]

El ejemplo 2.5.1 inspira la siguiente definición:

[5] Como en el ejemplo 1.2.4 (2), en este argumento hemos usado la unicidad de la descomposición de un número entero como producto de primos, hecho que suponemos conoces. Veremos esta propiedad con detalle en la sección 3.3, no solo para $\mathbf{Z}$ sino para toda una clase de anillos llamados *dominios de factorización única*.

Definición 2.5.2. Sea R un anillo y sea $\mathfrak{p}$ un ideal de R. Decimos que $\mathfrak{p}$ es *primo* si

(1) $\mathfrak{p} \neq (1)$; y

(2) para todo $x, y \in R$ tales que $xy \in \mathfrak{p}$ se tiene que, $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$.

Ejemplos 2.5.3. (1) Como vimos en el ejemplo 2.5.1 un ideal de $\mathbf{Z}$ generado por un número primo es un ideal primo. En cambio, un ideal de $\mathbf{Z}$ generado por un número compuesto no es primo. Por ejemplo, el ideal (6) no es un ideal primo, ya que $2 \cdot 3 = 6 \in (6)$ pero $2 \notin (6)$ y $3 \notin (6)$, pues ni 2 ni 3 son múltiplos enteros de 6.

(2) Un anillo R es un dominio de integridad si y solo si (0) es un ideal primo.

(3) Sea $\mathbf{k}$ un cuerpo y sea $R = \mathbf{k}[X]$. El ideal (X^2) no es primo ya que $X \cdot X = X^2 \in (X^2)$, pero $X \notin (X^2)$. Esto se puede razonar así. Si $X \in (X^2)$, entonces existiría $q \in \mathbf{k}[X]$ tal que

$$X = qX^2. \tag{2.5.3.1}$$

Como R es un dominio de integridad, de (2.5.3.1) tendríamos $1 = qX$, de donde X sería unidad, lo cual no es cierto, ya que las unidades de R son los polinomios constantes no nulos.

Otra forma de razonar es usando el grado: no se puede dar una ecuación como (2.5.3.1) ya que el término de la izquierda tiene grado 1 y el de la derecha tiene al menos grado 2.

(4) Sea $\mathbf{k}$ un cuerpo y sea $R = \mathbf{k}[X, Y]$. El ideal (XY) no es un ideal primo de R. En efecto, tenemos que $XY \in (XY)$ pero, argumentando como en (3), no es difícil ver que $X \notin (XY)$ e $Y \notin (XY)$.

Proposición 2.5.4. *Sea R un anillo e I un ideal de R. El ideal I es primo si y solo si el anillo cociente R/I es un dominio de integridad.*

Demostración. Veamos que I primo implica R/I dominio de integridad. Como $I \neq (1)$, $R/I \neq 0$. Sean $x, y \in R$, sean $\overline{x}, \overline{y}$ sus clases en R/I y supongamos que $\overline{x} \cdot \overline{y} = \overline{0}$. Entonces $\overline{xy} = \overline{0}$, que equivale a $xy \sim_I 0$, que equivale a $xy - 0 \in I$, que equivale a $xy \in I$. Como I es primo, tenemos que $x \in I$ o $y \in I$. En el primer caso $\overline{x} = \overline{0}$ y en el segundo $\overline{y} = \overline{0}$ en R/I.
Veamos que R/I dominio de integridad implica I primo. Como $R/I = 0$, tenemos que $I \neq (1)$. Sean $x, y \in R$ tales que $xy \in I$. Entonces $\overline{x} \cdot \overline{y} = \overline{xy} = \overline{0}$ en R/I. Como R/I es un dominio de integridad, $\overline{x} = \overline{0}$ o $\overline{y} = \overline{0}$. En el primer caso $x \in I$ y en el segundo $y \in I$. □

Ejemplos 2.5.5. (1) Sea R un dominio de integridad. El ideal (X) de $R[X]$ es primo. Esto es una consecuencia directa del ejemplo 2.4.3 y de la proposición 2.5.4.

También lo podemos comprobar directamente. Sean $g_1, g_2 \in R[X]$ y supongamos que $g_1, g_2 \notin (X)$. Eso quiere decir que los términos independientes a y b de g_1, g_2 son ambos no nulos. Como R es un dominio de integridad, $ab \neq 0$, por lo que el término independiente de $g_1 g_2$, que es ab, es no nulo. Esto implica que $g_1 g_2$ no es múltiplo de X, es decir, que $g_1 g_2 \notin (X)$.

(2) Sea R un dominio de integridad y sea $a \in R$. El ideal $(X - a)$ de $R[X]$ es primo. Esto es una consecuencia directa del ejemplo 2.4.4 y de la proposición 2.5.4.

(3) Si en (1) hacemos $R = \mathbf{Z}$, deducimos que el ideal (X) de $\mathbf{Z}[X]$ es primo.

(4) Sea $\mathbf{k}$ un cuerpo. Si en (1) hacemos $R = \mathbf{k}$, deducimos que el ideal (X) de $\mathbf{k}[X]$ es primo.

(5) Sea $\mathbf{k}$ un cuerpo. Si en (1) hacemos $R = \mathbf{k}[Y]$, deducimos que el ideal (X) de $\mathbf{k}[X, Y]$ es primo. Más en general, si $R = \mathbf{k}[X_2, \ldots, X_n]$, deducimos que el ideal (X_1) es de $\mathbf{k}[X_1, \ldots, X_n]$ es primo.

Ahora introducimos la noción de ideal *maximal*, que será un ideal de un anillo R para el cual no existe ningún ideal más grande que él, exceptuado el (1) (es decir, es un elemento maximal en el conjunto de los ideales de R distintos de (1) con respecto de la relación de contenido):

Definición 2.5.6. Sea R un anillo y sea $\mathfrak{m}$ un ideal de R. Decimos que $\mathfrak{m}$ es *maximal* si $\mathfrak{m} \neq (1)$ y, para todo ideal J de R, entonces

(i) o $\mathfrak{m} = J$,

(ii) o $J = (1)$.

Ejemplos 2.5.7. (1) Un anillo R es un cuerpo si y solo si el ideal (0) es maximal. Esto se deduce de manera inmediata del hecho de un anillo es un cuerpo si y solo si solo posee dos ideales, el ideal (0) y el ideal (1) (véase la proposición 2.1.12).

(2) El ideal (2) de $\mathbf{Z}$ es maximal. Obviamente $(2) \neq (1) = \mathbf{Z}$, ya que (2) es el conjunto formado por todos los enteros pares. Sea ahora J un ideal de $\mathbf{Z}$ tal que $(2) \subsetneq J$. Entonces existe un número impar n perteneciente a J, que es de la forma $m = 2n + 1$ para algún entero par n. Así $1 = m - 2n$. Como $m \in J$, $2n \in (2) \subsetneq J$ y J es un ideal, concluimos que $1 \in J$, de donde $J = (1)$.

(3) Sea $\mathbf{k}$ un cuerpo. El ideal (X) es un ideal maximal de $\mathbf{k}[X]$, el ideal (X, Y) es un ideal maximal de $\mathbf{k}[X, Y]$ y, en general, el ideal $(X_1, \ldots, X_n)$ es un ideal maximal de $\mathbf{k}[X_1, \ldots, X_n]$.

Lo argumentamos para el ideal (X, Y) de $\mathbf{k}[X, Y]$. Los elementos de (X, Y) son los polinomios de $\mathbf{k}[X, Y]$ con término independiente nulo. En particular eso implica

que $(X, Y) \neq (1)$. Sea ahora J un ideal de $\mathbf{k}[X, Y]$ tal que $(X, Y) \subsetneq J$. Entonces existe $g \in J$, $g \notin (X, Y)$, por lo que g tiene término independiente $a \in \mathbf{k}$, $a \neq 0$. Entonces g es de la forma $g = a + h$, siendo h un polinomio de $\mathbf{k}[X, Y]$ con término independiente nulo, es decir, $h \in (X, Y)$. Por tanto $a = g - h$ y, como $g \in J$ y $h \in (X, Y) \subsetneq J$ y J es un ideal, $a \in J$. Como $a \in \mathbf{k}$, $a \neq 0$, a es una unidad en $\mathbf{k}[X, Y]$, de donde $J = (1)$.

(4) El ideal $(2, X)$ de $\mathbf{Z}[X]$ es maximal. En efecto, $(2, X)$ es el conjunto de polinomios de $\mathbf{Z}[X]$ cuyo término independiente es par, por lo que en particular, $(2, X) \neq (1) = \mathbf{Z}[X]$. Por otra parte, si J es un ideal de $\mathbf{Z}[X]$ que contiene a $(2, X)$ estrictamente, existe un número impar de la forma $2n + 1$ para algún $n \in \mathbf{Z}$ y un polinomio $h \in \mathbf{Z}[X]$ tal que $g := 2n + 1 + h \cdot X$ pertenece a J. Entonces $1 = g - (2n + h \cdot X)$, por lo que $1 \in J$, ya que $g \in J$, $n \cdot 2 + h \cdot X \in (2, X) \subsetneq J$ y J es un ideal. De esto se sigue que $J = (1)$.

(5) El ideal (0) de $\mathbf{Z}$ no es maximal. Esto se puede ver directamente ya que podemos exhibir por ejemplo esta cadena de contenidos estrictos de ideales:

$$(0) \subsetneq (2) \subsetneq (1).$$

Otra forma de justificarlo es como consecuencia del primer ejemplo de esta lista, ya que $\mathbf{Z}$ no es un cuerpo.

(6) Sea $\mathbf{k}$ un cuerpo y sea $n \in \mathbf{N}$. Al igual que en (4), el ideal (0) de $\mathbf{k}[X_1, \ldots, X_n]$ no es maximal.

(7) Sea $\mathbf{k}$ un cuerpo. Los ideales (X) e (Y) de $\mathbf{k}[X, Y]$ no son maximales ya que tenemos estas cadenas de contenidos estrictos:

$$\begin{array}{ccccc} (X) & \subsetneq & (X, Y) & \subsetneq & (1) = \mathbf{k}[X, Y] \\ (Y) & \subsetneq & (X, Y) & \subsetneq & (1) = \mathbf{k}[X, Y] \ . \end{array}$$

(8) Los ideales (2) e (X) de $\mathbf{Z}[X]$ no son maximales ya que tenemos estas cadenas de contenidos estrictos:

$$\begin{array}{ccccc} (2) & \subsetneq & (2, X) & \subsetneq & (1) = \mathbf{Z}[X] \\ (X) & \subsetneq & (2, X) & \subsetneq & (1) = \mathbf{Z}[X] \end{array}$$

(comprueba que los contenidos son efectivamente estrictos).

(9) El ideal (6) de $\mathbf{Z}$ no es maximal, ya que tenemos la sigiente cadena de contenidos estrictos:

$$(6) \subsetneq (2) \subsetneq (1) = \mathbf{Z}.$$

Proposición 2.5.8. *Sea R un anillo y sea I un ideal de R. El ideal I es maximal si y solo si R/I es un cuerpo.*

Demostración. Vemos que I maximal implica R/I cuerpo. Como $I \neq (1)$, R/I es no nulo. Queremos ver que todo elemento no nulo de R/I tiene inverso. Sea $x \in R$, sea $\overline{x}$ su clase en R/I y supongamos $\overline{x} \neq \overline{0}$. Entonces $x \notin I$. Entonces $J = I + (x)$ es un ideal de R que contiene a I de manera estricta. Como I es maximal, tenemos que $J = (1)$, es decir, existe $z \in R$ e $y \in I$ tales que $1 = y + zx$. Entonces $xz = 1 - y$ y, como $y \in I$, tenemos que $\overline{y} = \overline{0}$, por lo que, tomando clases de equivalencia, tenemos

$$\overline{x} \cdot \overline{z} = \overline{xz} = \overline{1 - y} = \overline{1} - \overline{y} = \overline{1}.$$

Así pues $\overline{z}$ es el inverso de $\overline{x}$ con respecto al producto en R/I.

Veamos ahora que R/I cuerpo implica I maximal. En primer lugar $I \neq (1)$ pues si $R/I \neq 0$. Sea J un ideal de R que contiene estrictamente a I. Queremos ver que $J = (1)$. Entonces existe $x \in J$, $x \notin I$, por lo que $\overline{x} \neq \overline{0}$. Como R/I es un cuerpo, existe $z \in R$ tal que $\overline{z}$ es el inverso de $\overline{x}$ respecto del producto en R/I. Entonces $\overline{1} = \overline{x} \cdot \overline{z} = \overline{xz}$, es decir, existe $y \in I$ tal que $1 - xz = y$. Entonces $1 = y + zx$ está en J, ya que $y \in I \subsetneq J$, $x \in J$ y J es un ideal. Por tanto $J = (1)$. □

Ejemplos 2.5.9. (1) Los ideales (2), (3) y (5) de $\mathbf{Z}$ son maximales. En efecto, si hacemos la tabla del producto de $\mathbf{Z}/(2)$, $\mathbf{Z}/(3)$ y $\mathbf{Z}/(5)$ vemos que todos ellos son cuerpos. La afirmación se sigue entonces de la proposición 2.5.8. En el corolario 3.2.10 veremos que, si $p \in \mathbf{N}$, el ideal (p) es maximal si y solo si p es un número primo.

(2) Sea $\mathbf{k}$ un cuerpo y sea $a \in \mathbf{k}$. El ideal $(X - a)$ de $\mathbf{k}[X]$ es maximal. Esto es una consecuencia directa del ejemplo 2.4.4 y de la proposición 2.5.8

(3) Sea $\mathbf{k}$ un cuerpo. El ideal $(X_1, \ldots, X_n)$ de $\mathbf{k}[X_1, \ldots, X_n]$ es maximal, por el ejemplo 2.4.5 y la proposición 2.5.8. En cambio, si $n \geq 2$, el ideal (X_1) de $\mathbf{k}[X_1, \ldots, X_n]$ no es maximal, ya que, según el ejemplo 2.4.3, $\mathbf{k}[X_1, \ldots, X_n]/(X_1)$ es isomorfo a $\mathbf{k}[X_2, \ldots, X_n]$, que no es cuerpo.

(4) Del ejemplo 2.4.6 y de la proposición 2.5.8 se deduce que el ideal $(X^2 + 1)$ de $\mathbf{R}[X]$ es maximal.

(5) Aunque vimos en el ejemplo 2.5.7 que el ideal $(2, X)$ de $\mathbf{Z}[X]$ es maximal, esto también se deduce del ejemplo 2.4.7 y la proposición 2.5.8, ya que $\mathbf{Z}/(2)$ es un cuerpo.

También lo podemos ver así. Por el teorema 2.4.10 los anillos $\mathbf{Z}[X]/(2, X)$ y $\mathbf{Z}[X]/(X)/((2, X)/(X))$ son isomorfos. Por el ejemplo 2.4.3, $\mathbf{Z}[X]/(X)$ es isomorfo a $\mathbf{Z}$ y, vía ese isomorfismo, el ideal $(2, X)/(X)$ de $\mathbf{Z}[X]/(X)$ es isomorfo al ideal (2) de $\mathbf{Z}$. Entonces $\mathbf{Z}[X]/(X)/((2, X)/(X))$ es isomorfo a $\mathbf{Z}/(2)$.

En los ejemplos 2.5.3, 2.5.5, 2.5.7 y 2.5.9 hemos visto casos de ideales que son primos y maximales, como (2) en $\mathbf{Z}$ o (X) en $\mathbf{k}[X]$ y de ideales que son primos pero no maximales, como (2) y (X) en $\mathbf{Z}[X]$ o (X) en $\mathbf{k}[X, Y]$. Vemos a continuación la relación entre en concepto de ideal primo y el de ideal maximal.

Proposición 2.5.10. *Sea R un anillo y sea I un ideal de R. Si I es maximal, entonces I es primo.*

Demostración. Si I es maximal, entonces R/I es un cuerpo según la proposición 2.5.8. En ese caso, según el ejemplo 1.2.4 (4), R/I es un dominio de integridad. Por la proposición 2.5.4, I es un ideal primo. □

Observación 2.5.11. Como ya se ha indicado, el recíproco de la proposición 2.5.10 no es cierto. Por ejemplo, (X) es un ideal primo de $\mathbf{Z}[X]$ que no es maximal.

2.6 Teorema chino del resto

Terminamos el tema 2 con un resultado importante, el teorema chino del resto, llamado así porque, en su versión particular para números enteros, en el siglo III. Aunque la versión general es para un número finito arbitrario de ideales (véase por ejemplo el teorema II.2.5 en *Estructuras Algebraicas: Divisibilidad en Anillos Conmutativos*, de J.F. Fernando y J.M. Gamboa), aquí daremos una versión para dos ideales; para las aplicaciones que veremos en ejemplos y ejercicios nos bastará usar esta, utilizándola en caso necesario de manera repetida (de hecho, la versión general para un número arbitrario de ideales se puede obtener a partir del teorema 2.6.1 realizando una inducción adecuada).

Teorema 2.6.1. *Sea R un anillo y sean I y J dos ideales de R. Si I y J son coprimos, entonces la aplicación*

$$\begin{array}{rccc} \overline{\varphi}: & \frac{R}{IJ} = \frac{R}{I \cap J} & \longrightarrow & \frac{R}{I} \times \frac{R}{J} \\ & z + IJ & \mapsto & (z + I, z + J) \end{array}$$

está bien definida y es un isomorfismo de anillos.

Demostración. Definimos la aplicación

$$\begin{array}{rccc} \varphi: & R & \longrightarrow & \frac{R}{I} \times \frac{R}{J} \\ & x & \mapsto & (x + I, x + J). \end{array}$$

La aplicación φ es un homomorfismo porque las proyecciones canónicas de R a R/I y a R/J lo son y por la forma en que se definen las operaciones en un anillo producto.

El núcleo de φ está formado por los elementos x de R tales que $x + I = 0 + I$ y $x + J = 0 + J$, es decir, por los elementos x de R tales que $x \in I$ y $x \in J$. Por tanto el núcleo de φ es $I \cap J$, que es también IJ porque I y J son coprimos.

Vemos ahora que φ es sobreyectivo. Hallamos primero sendas preimágenes de $(1+I, 0+J)$ y $(0+I, 1+J)$. Como I y J son coprimos, existen $x \in I$ e $y \in J$ tales que $1 = x + y$. Como $x \in I$,

se tiene $x+I = 0+I$ y, tomando clases módulo I, obtenemos $1+I = y+I$. Análogamente, como $y \in J$, se tiene $y+J = 0+J$ y, tomando clases módulo J, obtenemos $1+J = x+I$. Entonces

$$\begin{aligned} \varphi(y) &= (1+I, 0+J) \\ \varphi(x) &= (0+I, 1+J) \end{aligned}$$

Sean ahora $z_1, z_2 \in R$ y sea $(z_1+I, z_2+J) \in R/I \times R/J$. Entonces

$$(z_1+I, z_2+J) = (z_1+I, z_1+J)(1+I, 0+J) + (z_2+I, z_2+J)(0+I, 1+J) = \\ \varphi(z_1)\varphi(y) + \varphi(z_2)\varphi(x) = \varphi(yz_1 + xz_2).$$

Así pues, todo elemento de $R/I \times R/J$ tiene una preimagen en R, por lo cual φ es sobreyectivo.

Aplicando el teorema 2.4.1, $\overline{\varphi}$ es un isomorfismo entre los anillos R/IJ y $R/I \times R/J$. □

Observación 2.6.2. La demostración del teorema 2.6.1 nos dice cómo es el isomorfismo inverso de $\overline{\varphi}$:

$$\overline{\varphi}^{-1}(z_1+I, z_2+J) = (yz_1 + xz_2) + IJ,$$

donde $x \in I, y \in J$ y $1 = x+y$.

Ejemplo 2.6.3. Los anillos $\mathbf{Z}/(30)$ y $\mathbf{Z}/(2) \times \mathbf{Z}/(3) \times \mathbf{Z}/(5)$ son isomorfos. Vemos primero que $\mathbf{Z}/(30)$ es isomorfo a $\mathbf{Z}/(6) \times \mathbf{Z}/(5)$. Para ello observamos que $1 = 1 \cdot 6 + (-1) \cdot 5$, de donde se sigue que los ideales (6) y (5) son coprimos. Por otra parte, según el ejercicio 2 (a) de la hoja 2, $(30) = (6)(5)$. Entonces el teorema 2.6.1 nos da un isomorfismo

$$\begin{array}{rccc} \overline{\varphi_1}: & \mathbf{Z}/(30) & \longrightarrow & \mathbf{Z}/(6) \times \mathbf{Z}/(5) \\ & x+(30) & \mapsto & (x+(6), x+(5)). \end{array}$$

Observamos ahora que $1 = (-1) \cdot 2 + 1 \cdot 3$, de donde se deduce que los ideales (2) y (3) son coprimos. Por otra parte, según el ejercicio 2 (a) de la hoja 2, $(6) = (2)(3)$. Usando el teorema 2.6.1 podemos construir un isomorfismo

$$\begin{array}{rccc} \overline{\varphi_2}: & \mathbf{Z}/(6) \times \mathbf{Z}/(5) & \longrightarrow & \mathbf{Z}/(2) \times \mathbf{Z}/(3) \times \mathbf{Z}/(5) \\ & (x+(6), x+(5)) & \mapsto & (x+(2), x+(3), x+(5)). \end{array}$$

Componiendo $\overline{\varphi_1}$ y $\overline{\varphi_2}$ obtenemos el isomorfismo $\overline{\varphi} = \overline{\varphi_2} \circ \overline{\varphi_1}$ deseado:

$$\begin{array}{rccc} \overline{\varphi}: & \mathbf{Z}/(30) & \longrightarrow & \mathbf{Z}/(2) \times \mathbf{Z}/(3) \times \mathbf{Z}/(5) \\ & x+(30) & \mapsto & (x+(2), x+(3), x+(5)). \end{array}$$

El isomorfismo $\overline{\varphi}$ hace más trasparente la estructura de $\mathbf{Z}/(30)$. Al identificarlo con un producto de anillos, vemos claramente que $\mathbf{Z}/(30)$ no es un dominio de integridad. También nos ayuda a contar fácilmente las unidades de $\mathbf{Z}/(30)$, pues, según la observación 2.3.6, estas se corresponden vía $\overline{\varphi}$ con las unidades de $\mathbf{Z}/(2) \times \mathbf{Z}/(3) \times \mathbf{Z}/(5)$. Según el ejercicio 3 (b) de la hoja 1, las unidades de $\mathbf{Z}/(2) \times \mathbf{Z}/(3) \times \mathbf{Z}/(5)$ son el conjunto

$U(\mathbf{Z}/(2))\times U(\mathbf{Z}/(3))\times U(\mathbf{Z}/(5))$. Como $\mathbf{Z}/(2)$, $\mathbf{Z}/(3)$ y $\mathbf{Z}/(5)$ son cuerpos (se puede ver directameante haciendo sus tablas del producto), el cardinal de $U(\mathbf{Z}/(2))\times U(\mathbf{Z}/(3))\times U(\mathbf{Z}/(5))$ es $1\cdot 2\cdot 4 = 8$. Por tanto $\mathbf{Z}/(30)$ tiene 8 unidades (véase la proposición 3.2.13).

Vemos también como $\overline{\varphi}$ nos permite decidir si un elemento concreto de $\mathbf{Z}/(30)$ es unidad y cuál es su inverso. Como

$$\overline{\varphi}(17+(30)) = (17+(2), 17+(3), 17+(5)) = (1+(2), 2+(3), 2+(5))$$

y $1+(2), 2+(3), 2+(5)$ son unidades respectivamente en $\mathbf{Z}/(2)$, $\mathbf{Z}/(3)$ y $\mathbf{Z}/(5)$, concluimos que $\overline{17}$ es una unidad de $\mathbf{Z}/(30)$. El inverso de $(1+(2), 2+(3), 2+(5))$ en $\mathbf{Z}/(2)\times\mathbf{Z}/(3)\times\mathbf{Z}/(5)$ es $(1+(2), 2+(3), 3+(5))$. Por la proposición 2.1.2 (3) el inverso de $17+(30)$ en $\mathbf{Z}/(30)$ es

$$\overline{\varphi}^{-1}(1+(2), 2+(3), 3+(5)).$$

Como $1 = (-2)+3$, la observación 2.6.2 nos dice que

$$\overline{\varphi}_2^{-1}(1+(2), 2+(3), 3+(5)) = (3\cdot 1+(-2)\cdot 2)+(6), 3+(5)) = (-1+(6), 3+(5)).$$

Como $1 = 6+(-5)$, la observación 2.6.2 nos dice que

$$\overline{\varphi}_1^{-1}(-1+(6), 3+(5)) = ((-5)\cdot(-1)+6\cdot 3)+(6)) = 23+(30).$$

Entonces

$$\overline{\varphi}^{-1}(1+(2), 2+(3), 3+(5)) = \overline{\varphi}_1^{-1}\left(\overline{\varphi}_2^{-1}(1+(2), 2+(3), 3+(5))\right) = 23+(30). \tag{2.6.3.1}$$

Así pues, el inverso de $\overline{17}$ en $\mathbf{Z}/(30)$ es $\overline{23}$ (si quieres hacer la comprobación de que efectivamente es así, puedes hacer la división de $17\cdot 23$ entre 30 y ver que el resto es 1).

Ejemplo 2.6.4. Sea $\mathbf{k}$ un cuerpo y sean $a, b \in \mathbf{k}$, $a \neq b$. Entonces la aplicación

$$\begin{array}{rccc} \phi: & \dfrac{\mathbf{k}[X]}{((X-a)(X-b))} & \longrightarrow & \mathbf{k}\times\mathbf{k} \\ & f(X)+((X-a)(X-b)) & \mapsto & (f(a), f(b)) \end{array}$$

está bien definida y es un isomorfismo de anillos.

Para verlo consideramos los ideales $(X-a)$ y $(X-b)$ de $\mathbf{k}[X]$. Los elementos de $(X-a)$ son los polinomios de $\mathbf{k}[X]$ que se anulan en a. De igual forma, los elementos de $(X-b)$ son los polinomios de $\mathbf{k}[X]$ que se anulan en b. Los ideales $(X-a)$ y $(X-b)$ son coprimos, ya que $X-b \notin (X-a)$, puesto que, como $a \neq b$, $X-b$ no se anula en a; entonces $(X-a) \subsetneq (X-a)+(X-b)$ y, como $(X-a)$ es maximal por el ejemplo 2.5.9 (2), $(X-a)+(X-b) = (1)$. Entonces por el teorema 2.6.1

$$\begin{array}{rccc} \overline{\varphi}: & \dfrac{\mathbf{k}[X]}{((X-a)(X-b))} & \longrightarrow & \dfrac{\mathbf{k}[X]}{(X-a)}\times\dfrac{\mathbf{k}[X]}{(X-b)} \\ & f(X)+((X-a)(X-b)) & \mapsto & (f(X)+(X-a), f(X)+(X-b)). \end{array}$$

Por el ejemplo 2.4.4 y el ejercicio 5 de la hoja 2, tenemos un isomorfismo

$$\begin{array}{rccc} \overline{\varphi_a} \times \overline{\varphi_b} : & \dfrac{\mathbf{k}[X]}{(X-a)} \times \dfrac{\mathbf{k}[X]}{(X-b)} & \longrightarrow & \mathbf{k} \times \mathbf{k} \\ & (f(X) + (X-a), f(X) + (X-b)) & \mapsto & (f(a), f(b)). \end{array}$$

El isomorfismo buscado es la composición $\phi = (\overline{\varphi_a} \times \overline{\varphi_b}) \circ \overline{\varphi}$. Observamos que $\phi = (\varphi_a, \varphi_b)$. La interpretación geométrica de $\overline{\varphi}$ es la siguiente. Por la proposición 2.1.26 y el ejercicio 2 (a) de la hoja 2, $((X-a)(X-b)) = (X-a) \cap (X-b)$ por lo que el ideal es el conjunto de los polinomios de $\mathbf{k}[X]$ que se anulan en a y en b. Entonces, dos polinomios $f(X)$ y $g(X)$ tienen la misma clase módulo $((X-a)(X-b))$ si y solo si $f(X)-g(X)$ pertenece a $((X-a)(X-b))$, es decir, si $f(X)-g(X)$ se anula en a y b, es decir, si $f(a) = g(a)$ y $f(b) = g(b)$. Parece lógico pues identificar cada clase de equivalencia en $\dfrac{\mathbf{k}[X]}{((X-a)(X-b))}$ de un polinomio $f(X)$ con el par de valores $(f(a), f(b))$ que $f(X)$ toma en a y b. Esta identificación es precisamente la que nos da el isomorfismo ϕ que hemos construido antes.

Por otra parte la interpretación del isomorfismo inverso ϕ^{-1} es esta. Dado un par $(\alpha, \beta) \in \mathbf{k} \times \mathbf{k}$, $\phi^{-1}(\alpha, \beta)$ es una clase de equivalencia de $\dfrac{\mathbf{k}[X]}{((X-a)(X-b))}$ cuyos elementos son los polinomios de $\mathbf{k}[X]$ que valen α al ser evaluados en a y β al ser evaluados en b. Así pues, ϕ^{-1} resuelve el problema de *interpolación polinómica* por los puntos (a, α) y (b, β) de $\mathbf{k}^2$.

Ilustramos lo anterior en un caso concreto: $\mathbf{k} = \mathbf{R}$, $a = 1, b = -1, \alpha = 2, \beta = 3$. Tenemos $1 = (-1/2)(X-1) + (1/2)(X+1)$. Por la observación 2.6.2

$$\phi^{-1}(2,3) = 2(1/2)(X+1) + 3(-1/2)(X-1) = -1/2X + 5/2 + (X^2+1).$$

Eso quiere decir que los polinomios de $\mathbf{R}[X]$ que valen 2 en el punto 1 y 3 en el punto -1 son de la forma $-1/2X + 5/2 + q(X)(X^2+1)$, donde $q(X)$ es un polinomio cualquiera de $\mathbf{R}[X]$. Entonces, el polinomio de menor grado de $\mathbf{R}[X]$ que vale 2 en el punto 1 y 3 en el punto -1 es $-1/2X + 5/2$.

Ejemplo 2.6.5. Usando el teorema 2.6.1 repetidamente y el ejemplo 2.4.4, se puede resolver el problema de interpolación polinómica para un número arbitrario n de puntos de $\mathbf{k}^n$.

Para verlo, consideramos $a_1, a_2, \ldots, a_n$ elementos distintos de un cuerpo $\mathbf{k}$. Podemos probar por inducción que, para todo $2 \leq \ldots k \leq n$, los siguientes ideales de $\mathbf{k}[X]$ cumplen:

(i) $((X-a_1)(X-a_2)\cdots(X-a_{k-1}))$ y $(X-a_k)$; y son coprimos

(ii) $(X-a_1) \cap (X-a_2) \cap \cdots \cap (X-a_{k-1}) = ((X-a_1)(X-a_2)\cdots(X-a_{k-1}))$.

En efecto, si $k = 2$, demostramos la afirmación (i) en el ejemplo 2.6.4 mientras que (ii) es trivial. Supongamos el resultado cierto para $2 \leq k < n$ y demostrémoslo para $k+1$. Por hipótesis de inducción, la afirmación (i) se cumple para k, por lo que, por

la proposición 2.1.26, $(X-a_1)\cap(X-a_2)\cap\cdots\cap(X-a_k)=((X-a_1)(X-a_2)\cdots(X-a_k))$, que es la afirmación (ii) para $k+1$. De ahí se deduce que $((X-a_1)(X-a_2)\cdots(X-a_k))$ es el conjunto formado por los polinomios de $\mathbf{k}[X]$ que se anulan en $a_1,a_2,\ldots,a_k$. Como $a_1,a_2,\ldots,a_k,a_{k+1}$ y el polinomio $(X-a_1)(X-a_2)\cdots(X-a_k)$ tiene grado k y se anula en $a_1,a_2,\ldots,a_k$, entonces, por el ejercicio 9, el polinomio $(X-a_1)(X-a_2)\cdots(X-a_k)$ no se anula en a_{k+1}, por lo que

$$((X-a_{k+1}))\subsetneq((X-a_{k+1}))+((X-a_1)(X-a_2)\cdots(X-a_k)).$$

Como, por el ejemplo 2.5.9 (2), el ideal $((X-a_{k+1}))$ es maximal, tenemos que

$$((X-a_{k+1}))+((X-a_1)(X-a_2)\cdots(X-a_k))=(1),$$

con lo que queda demostrada la afirmación (i) para $k+1$.

Podemos aplicar el teorema 2.6.1 repetidas veces y obtener un isomorfismo

$$\begin{array}{rccc}\overline{\varphi}: & \dfrac{\mathbf{k}[X]}{((X-a_1)(X-a_2)\cdots(X-a_n))} & \longrightarrow & \dfrac{\mathbf{k}[X]}{(X-a_1)}\times\cdots\times\dfrac{\mathbf{k}[X]}{(X-a_n)}\\ & f(X)+((X-a_1)(X-a_2)\cdots(X-a_n)) & \mapsto & (f(X)+(X-a_1),\ldots f(X)+(X-a_n)).\end{array}$$

Componiendo $\overline{\varphi}$ con el isomorfismo $\overline{\varphi_{a_1}}\times\overline{\varphi_{a_2}}\times\cdots\times\overline{\varphi_{a_n}}$, donde $\overline{\varphi_{a_k}}$ es el isomorfismo que aparece en el ejemplo 2.4.4 para $a=a_k$, obtenemos un isomorfismo

$$\begin{array}{rccc}\phi: & \dfrac{\mathbf{k}[X]}{((X-a_1)(X-a_2)\cdots(X-a_n))} & \longrightarrow & \mathbf{k}\times\overset{n)}{\cdots}\times\mathbf{k}\\ & f(X)+((X-a_1)(X-a_2)\cdots(X-a_n)) & \mapsto & (f(a_1),f(a_2),\ldots,f(a_n)),\end{array}$$

que no es sino $\phi=\varphi_{a_1}\times\varphi_{a_2}\times\cdots\times\varphi_{a_n}$, donde φ_{a_k} es el homomofismo de evaluación en a_k.

Dados $\alpha_1,\alpha_2,\ldots,\alpha_n\in\mathbf{k}$, la imagen inversa $\phi^{-1}(\alpha_1,\alpha_2,\ldots,\alpha_n)$ es una clase de equivalencia de

$$\frac{\mathbf{k}[X]}{((X-a_1)(X-a_2)\cdots(X-a_n))},$$

que está formada por los polinomios de $\mathbf{k}[X]$ que, para todo $k=1,2,\ldots,n$, toman el valor α_k al ser evaluados en a_k.

Tema 3

Divisibilidad

En $\mathbf{Z}$ estamos familiarizados con el concepto de divisibilidad. En este tema extendemos este concepto a cualquier dominio de integridad, distinguiendo entre varias clases de dominios, progresivamente más generales, según unas u otras propiedades de los números enteros se cumplan en estos dominios.

Definición 3.0.1. Sea R un dominio de integridad y sean $x, y \in R$, $y \neq 0$. Decimos que y *divide* a x o que x es *múltiplo* de y o que x es *divisible* por y si existe $z \in R$ tal que $x = z \cdot y$.

3.1 Dominios euclídeos

En los temas anteriores dimos por conocido que tanto en $\mathbf{Z}$ (recordemos el ejemplo 1.1.19) como en un anillo de polinomios en una variable con coeficientes en un cuerpo (recordemos los ejercicios 12 y 13 del tema 2 y el ejemplo 2.4.6) se puede dividir. Aun así vamos ahora a justificar con detalle la existencia de división en dichos anillos:

Teorema 3.1.1. *Sea $d \in \mathbf{Z}$ un entero no nulo. Para cada entero $m \in \mathbf{Z}$ existen $q, r \in \mathbf{Z}$ únicos, que llamaremos respectivamente cociente y resto de dividir m entre d, tales que $m = dq + r$ y $0 \leq r < |d|$.*

Demostración. Existencia de cociente y resto: Dividimos el argumento en varios casos.

Caso 1: $m \geq 0$ y $d > 0$. Si $0 \leq m < d$, como $m = 0 \cdot d + m$, podemos tomar $q = 0$ y $r = m$. Sea ahora $m \geq d$. Razonamos usando inducción completa sobre m. Si $m = d$, entonces $m = d \cdot 1 + 0$, por lo que el teorema se cumple en este caso. Supongamos que el teorema es cierto para todo $n \in \mathbf{Z}$ tal que $d < n < m$. Entonces, como $0 \leq m - d < m$, el teorema se cumple para $m - d$ y existen $q', r \in \mathbf{Z}$ tales que $m - d = dq' + r$ y $0 \leq r < d$. Así $m = d(q' + 1) + r$ y podemos tomar $q' + 1$ como cociente y r como resto de dividir m entre d.

Caso 2: $m < 0$ y $d > 0$. En este caso $-m > 0$, así que, por el caso 1, existen $q, r \in \mathbf{Z}$ tales que $-m = dq + r$ y $0 \leq r < d$. Si $r = 0$, $m = d(-q) + r$ y el teorema se cumple. Si $r > 0$,

entonces $0 < d - r < d$; como $m = d(-q) - r$, se tiene $m = d(-q-1) + (d-r)$ y podemos tomar $-q-1$ como cociente y $d-r$ como resto de dividir m entre d.

Caso 3: $d < 0$. Por los dos casos anteriores, el teorema se cumple para m y $-d$, es decir, existen $q, r \in \mathbf{Z}$ tales que $m = (-d)q + r$ y $0 \leq r < -d = |d|$. Entonces $m = d(-q) + r$ y podemos tomar $-q$ como cociente y r como resto de dividir m entre d.

Unicidad de cociente y resto: Sean $m, d \in \mathbf{Z}$, $d \neq 0$, $m = dq_1 + r_1$ y $m = dq_2 + r_2$ con $q_1, q_2, r_1, r_2 \in \mathbf{Z}$ y $0 \leq r_1, r_2 < |d|$. Entonces $d(q_1 - q_2) = (r_1 - r_2)$. Como $0 \leq r_1, r_2 < |d|$, tenemos $|r_1 - r_2| < |d|$. Como $d(q_1 - q_2) = (r_1 - r_2)$, se tiene entonces $|d| \cdot |q_1 - q_2| = |r_1 - r_2| < |d|$. Como $d \neq 0$, $|d| > 0$ y dividiendo por $|d|$ obtenemos $|q_1 - q_2| < 1$ y, al ser q_1, q_2 enteros, $|q_1 - q_2| = |r_1 - r_2| = 0$, con lo que $q_1 - q_2 = r_1 - r_2 = 0$, es decir, $q_1 = q_2$ y $r_1 = r_2$. □

Teorema 3.1.2. *Sea* $\mathbf{k}$ *un cuerpo. Sea* $g \in \mathbf{k}[X]$ *un polinomio no nulo. Para cada polinomio* $f \in \mathbf{k}[X]$ *existen polinomios* $q, r \in \mathbf{k}[X]$ *únicos, que llamaremos respectivamente cociente y resto de dividir* f *entre* g*, tales que* $f = gq + r$ *y* $gr(r) < gr(g)$.

Demostración.

Existencia de cociente y resto: Caso 1: $gr(f) < gr(g)$. Entonces $f = g \cdot 0 + f$, por lo que podemos tomar 0 como cociente y f como resto de dividir f entre g.

Caso 2: $gr(f) \geq gr(g)$. Razonamos por inducción completa sobre el grado de f. Sean $m = \text{gr}(f) \geq \text{gr}(g) = l$. Entonces $f = a_0 + a_1X + \cdots a_mX^m$ y $g = b_0 + b_1X + \cdots b_lX^l$, con $a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_l \in \mathbf{k}$ y $b_l \neq 0$. Entonces el grado de $f - b_l^{-1}a_mX^{m-l} \cdot g$ es menor que el grado de f y, por la hipótesis de inducción y el caso 1, existen $q, r \in \mathbf{k}[X]$ tales $f - (b_l^{-1}a_mX^{m-l} \cdot g) = gq + r$ y $\text{gr}(r) < \text{gr}(g)$. Entonces $f = g(q + b_l^{-1}a_mX^{m-l}) + r$, por lo que podemos tomar $q + b_l^{-1}a_mX^{m-l}$ como cociente y r como resto de dividir f entre g.

Unicidad de cociente y resto: Sean $f, g \in \mathbf{k}[X]$, $g \neq 0$, $f = gq_1 + r_1$ y $f = gq_2 + r_2$ con $q_1, q_2, r_1, r_2 \in \mathbf{k}[X]$ y $\text{máx}(\text{gr}(r_1), \text{gr}(r_2)) < \text{gr}(g)$. Entonces $g(q_1 - q_2) = (r_1 - r_2)$. Si $q_1 - q_2 \neq 0$, se sigue del ejercicio 9 (a) del tema 1 que $\text{gr}(g) \leq \text{gr}(r_1 - r_2) \leq \text{máx}(\text{gr}(r_1), \text{gr}(r_2)) < \text{gr}(g)$, lo cual es imposible. Entonces $q_1 - q_2 = 0 = r_1 - r_2$. □

Basándonos en los argumentos de la demostración del teorema 3.1.2 se puede dar el *algoritmo de división* en $\mathbf{k}[X]$. Como suponemos que, en la práctica, el manejo de ese algoritmo es sobradamente conocido, no lo detalleremos aquí en general sino que solo lo ilustraremos con el siguiente ejemplo:

Ejemplo 3.1.3. Consideramos los polinomios $f = 2X^4 - X^3 + X - 2$ y $g = 3X^2 + X + 1$ de $\mathbf{Q}[X]$. Hallamos el cociente y el resto de dividir f entre g así (escribimos en un color distinto cada sumando del cociente y, en el mismo color, el resultado de multiplicar

dicho sumando con el divisor):

$$
\begin{array}{rrrrr|l}
2X^4 - & X^3 + & & X - 2 & & 3X^2 + X + 1 \\ \cline{6-6}
2X^4 + & \frac{2}{3}X^3 + & \frac{2}{3}X^2 & & & \frac{2}{3}X^2 - \frac{5}{9}X - \frac{1}{27} \\ \cline{1-3}
 & -\frac{5}{3}X^3 - & \frac{2}{3}X^2 + & X - 2 & & \\
 & -\frac{5}{3}X^3 - & \frac{5}{9}X^2 - & \frac{5}{9}X & & \\ \cline{2-4}
 & & -\frac{1}{9}X^2 + & \frac{14}{9}X - 2 & & \\
 & & -\frac{1}{9}X^2 - & \frac{1}{27}X - \frac{1}{27} & & \\ \cline{3-4}
 & & & \frac{43}{27}X - \frac{53}{27} & &
\end{array}
$$

El cociente es $\frac{2}{3}X^2 - \frac{5}{9}X - \frac{1}{27}$ y el resto es $\frac{43}{27}X - \frac{53}{27}$.

Acabamos de ver en los teoremas 3.1.1 y 3.1.2 que en los dominios de integridad $\mathbf{Z}$ y $\mathbf{k}[X]$ existe división. Como era de esperar esto va a implicar que, por esa razón, $\mathbf{Z}$ y $\mathbf{k}[X]$ tengan propiedades comunes. Vamos pues a estudiar no solo $\mathbf{Z}$ y $\mathbf{k}[X]$ sino todos aquellos dominios de integridad en los que se pueda dividir.

Definición 3.1.4. Sea R un dominio de integridad y sea δ una función

$$\delta : R \setminus \{0\} \to \mathbf{N} \cup \{0\}.$$

Decimos que R es un *dominio euclídeo* con respecto a δ si se cumple lo siguiente:

(1) Para todo $x, y \in R$, $x, y \neq 0$, si x divide a y, entonces $\delta(x) \leq \delta(y)$.

(2) Para todo $x, y \in R$, $y \neq 0$, existen $q, r \in R$ tales que $x = yq + r$ donde, o bien $r = 0$, o bien $r \neq 0$ y $\delta(r) < \delta(y)$.

Ejemplos 3.1.5. (1) El teorema 3.1.1 nos dice que, si en $\mathbf{Z}$ tomamos como δ la función definida por el valor absoluto, entonces se cumple (2) de la definición 3.1.4. Como el valor absoluto también cumple (1) la definición 3.1.4, $\mathbf{Z}$ es un dominio euclídeo tomando como δ la función definida por el valor absoluto.

(2) El teorema 3.1.2 nos dice que, tomando como δ la función que asigna a cada polinomio su grado, se cumple (2) de la definición 3.1.4. Por otra parte del ejercicio 10 (a) del tema 1 se sigue (1) la definición 3.1.4. Por tanto $\mathbf{k}[X]$ es un dominio euclídeo para esta función δ.

Por supuesto $\mathbf{Z}$ y $\mathbf{k}[X]$ ($\mathbf{k}$ cuerpo) son los ejemplos más importantes de dominios euclídeos, pero hay otros:

Ejemplos 3.1.6. (1) Un cuerpo $\mathbf{k}$ es trivialmente un dominio euclídeo ya que la división de x entre y ($y \neq 0$) es siempre exacta, por lo que podemos tomar como δ la función constante 1.

(2) Veremos en el ejercicio 5 de la hoja 3 que $\mathbf{Z}[i]$ (los enteros de Gauss) son también un dominio euclídeo.

(3) Los subanillos $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$ y $\mathbf{Z}[\sqrt{-2}]$ de $\mathbf{C}$ son dominios euclídeos[1]

Observación 3.1.7. (1) Hacemos notar que la definición 3.1.4 no pide que q y r sean únicos. En el caso de $\mathbf{k}[X]$ cuando tomamos como δ el grado, el teorema 3.1.2 sí nos asegura que q y r son únicos. En cambio en $\mathbf{Z}$ con δ el valor absoluto, q y r no son únicos, ya que si q y r son los que aparecen en el enunciado del teorema 3.1.1, si $r \neq 0$, $r' = r - d$ y $q' = q + 1$ también cumplen (2) de la definición 3.1.4. La razón de que q y r sean únicos en el teorema 3.1.1 es que allí se les pide no solo que cumplan (2) de la definición 3.1.4 sino también que se cumpla $r \geq 0$. Asimismo, tampoco hay unos únicos q y r en la división euclídea que definiremos en $\mathbf{Z}[i]$ (véase el ejercicio 5 de la hoja 3). La existencia de una división con un cociente y un resto único tiene consecuencias muy útiles, tal y como veremos en las proposiciones 3.2.13 y 3.2.18.

(2) Un dominio euclídeo lo es con respecto a varias funciones δ. En efecto, si R es un dominio euclídeo y δ cumple (1) y (2) de la definición, para todo $\lambda \in \mathbf{N}$, la función $\lambda\delta$ también cumple (1) y (2).

Definición 3.1.8. Sea R un dominio de integridad. Decimos que dos elementos no nulos x e y de R están *asociados* si x divide a y e y divide a x.

Observación 3.1.9. Sean x e y dos elementos de un dominio de integridad R. Las siguientes afirmaciones son equivalentes:

(1) Los elementos x e y están asociados.

(2) Existe una unidad u de R tal que $y = ux$.

(3) Existe una unidad v de R tal que $x = vy$.

(4) Los ideales (x) e (y) son iguales.

Ejercicio 3.1.10. Sea R un dominio de integridad. "Estar asociado a" es una relación de equivalencia en $R \setminus \{0\}$.

Determinar las unidades de un anillo R es en general un problema complicado, pero cuando R es un dominio euclídeo la tarea resulta algo más fácil:

Proposición 3.1.11. *Sea R un dominio euclídeo con respecto a la función δ.*

(1) Se tiene que $\delta(1) = \text{mín}\,\{\delta(x) \mid x \in R \setminus \{0\}\}$.

(2) Un elemento $u \in R$ no nulo es una unidad si y solo si $\delta(u) = \delta(1)$.

(3) Dos elementos $x, y \in R$ están asociados si y solo si $\delta(x) = \delta(y)$ y, además, x divide a y.

[1] véanse los ejemplos IV.1.9 (4) y (5) del libro *Estructuras Algebraicas: Divisibilidad en Anillos Conmutativos*, de J. F. Fernando y J.M. Gamboa.

Demostración. Sea $x \in R$. Como 1 divide a x, la condición (1) de la definición 3.1.4 implica que $\delta(1) \leq \delta(x)$. Esto demuestra (1).

Si u es una unidad en R, entonces existe $u^{-1} \in R$ tal que $1 = uu^{-1}$, es decir, u divide a 1, por lo que $\delta(u) \leq \delta(1) \leq \delta(u)$, por la condición (1) de la definición 3.1.4 y el apartado (1) de esta proposición. Sea ahora $u \in R$ no nulo tal que $\delta(u) = \delta(1)$. Si dividimos 1 entre u obtenemos $1 = uv + r$, donde o bien $r = 0$, o bien $\delta(r) < \delta(u) = \delta(1)$. Como $\delta(1) \leq \delta(r)$ por el apartado (1), ha de ser $r = 0$. Por lo tanto $uv = 1$ y u es una unidad. Con esto completamos la demostración del apartado (2).

Sean x e y dos elementos no nulos de R. Entonces x e y están asociados si y solo si x divide a y e y divide a x. Esto implica $\delta(x) \leq \delta(y)$ y $\delta(x) \leq \delta(y)$, de donde $\delta(x) = \delta(y)$. Supongamos ahora que x divide a y y que $\delta(x) = \delta(y)$. Existe entonces $z \in R$ tal que $y = xz$. Dividiendo x entre y obtenemos $x = yq + r$, donde o bien $r = 0$, o bien $\delta(r) < \delta(y)$. Si ocurriera lo segundo, como $r = x - yq = x - xzq = x(1 - zq)$, entonces x dividiría a r, por lo que $\delta(x) \leq \delta(r) < \delta(y) = \delta(x)$, lo cual es absurdo. Por tanto $r = 0$ y $x = yq$, por lo que y divide a x, lo que, junto con la hipótesis de que x divide a y implica que x e y están asociados. Esto completa la prueba del apartado (3). □

3.2 Dominios de ideales principales

Todos los ejemplos de ideales de $\mathbf{Z}$ que hemos visto hasta ahora podían ser generados por un solo elemento. A continuación vemos que esto no ocurre por casualidad.

Definición 3.2.1. Sea R un anillo.

(1) Decimos que un ideal I de R es *principal* si existe $x \in R$ tal que $I = (x)$.

(2) Decimos que un dominio de integridad R es un *dominio de ideales principales* si todo ideal I de R es principal.

Teorema 3.2.2. *Sea R un dominio euclídeo con respecto a la función δ y sea I un ideal no nulo de R. Sea $l = \min\{\delta(x) \mid x \in I, x \neq 0\}$. Entonces I es principal e $y \in I$ es tal que $I = (y)$ si y solo si $\delta(y) = l$. En particular, R es un dominio de ideales principales.*

Demostración. Sea I ideal de R, $I \neq (0)$. En ese caso $\Sigma = \{\delta(x) \mid x \in I, x \neq 0\}$ es un subconjunto no vacío de $\mathbf{N} \cup \{0\}$, por lo que Σ tiene un elemento mínimo l. Sea $y \in I$ tal que $\delta(y) = l$. Veamos que $I = (y)$. En efecto: si $x \in I$, como R es un dominio euclídeo, entonces existen $q, r \in R$ tales que $x = yq + r$ y, o bien $r = 0$, o bien $\delta(r) < \delta(y)$. Entonces $r = x - qy \in I$, ya que $x, y \in I$ e I es un ideal. Si $r \neq 0$, entonces $\delta(r) < \delta(y)$ contradiría la minimalidad de $\delta(y)$. Por tanto, $r = 0$ y $x = qy$. Por otra parte, si $I = (y)$ y $x \in I, x \neq 0$, entonces $x = zy$ y por la condición (1) de la definición 3.1.4, $\delta(y) \leq \delta(x)$.

Acabamos de ver que, si R es un dominio euclídeo, entonces todo ideal no nulo de R es principal. Por otra parte, el ideal (0) de R es, obviamente, principal, por lo que queda

demostrado que, si R es un dominio euclídeo, entonces R es un dominio de ideales principales. □

Ejemplos 3.2.3. (1) Como corolario del teorema 3.2.2 se tiene, pues, que todos los dominios de integridad que aparecen en los ejemplos 3.1.5 y 3.1.6 son dominios de ideales principales. Por tanto los cuerpos (que un cuerpo $\mathbf{k}$ es un dominio de ideales principales se puede ver directamente, ya que los únicos ideales de $\mathbf{k}$ son (0) y (1), que son principales), el anillo $\mathbf{Z}$ de los números enteros, el anillo $\mathbf{k}[X]$ de polinomios en una variable con coeficientes en un cuerpo $\mathbf{k}$ y los anillos $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$ y $\mathbf{Z}[\sqrt{-2}]$ son dominios de ideales principales.

(2) En cambio, hay dominios de ideales principales que no son dominios euclídeos, como el subanillo $\mathbf{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ del cuerpo $\mathbf{C}$ de los números complejos[2]. La dificultad de este y otros ejemplos[3] excede el nivel de esta asignatura.

Observación 3.2.4. Los ejemplos 3.2.3 (2) muestran que el recíproco del teorema 3.2.2 es falso, es decir, la noción de dominio de ideales principales es más general que la noción de dominio euclídeo, ya que no todo dominio de ideales principales es euclídeo.

Ejemplos 3.2.5. (1) El dominio de integridad $\mathbf{Z}[X]$ no es un dominio de ideales principales, ya que, por ejemplo, el ideal $I = (2, X)$ no es principal. En efecto, si I fuera principal, entonces existiría un polinomio f de $\mathbf{Z}[X]$ tal que $I = (f)$. Entonces existiría $g \in \mathbf{Z}[X]$ tal que $2 = g \cdot f$. Como $\mathbf{Z}$ es un dominio de integridad, se sigue del ejercicio 10 (a) del tema 1 que f tiene grado 0, es decir, f es un polinomio constante $a \in \mathbf{Z}, a \neq 0$. Por otra parte, existiría $h \in \mathbf{Z}[X]$ de grado 1, es decir, de la forma $h = b_0 + b_1X$, con $b_0, b_1 \in \mathbf{Z}$, $b_1 \neq 0$, tal que $X = a \cdot h$. Entonces $ab_1 = 1$, por lo que $f \in U(\mathbf{Z}[X])$, de donde se seguiría que $I = (1)$. Esto es una contradicción, ya que el ideal $(2, X)$ es el ideal formado por los polinomios con término independiente par, por lo que, en particular, $I \neq (1)$.

(2) Sea $\mathbf{k}$ un cuerpo. El dominio de integridad $\mathbf{k}[X, Y]$ no es un dominio de ideales principales, ya que, por ejemplo, el ideal $I = (X, Y)$ no es principal. Razonando como en el ejemplo anterior, si I fuera principal, estaría generado por un polinomio $f \in \mathbf{k}[X, Y]$ que dividiría a X e Y. Considerando el grado en la variable X, se deduce que $f \in \mathbf{k}[Y]$. Como f dividiría a Y en $\mathbf{Z}[X, Y]$, considerando el grado en la variable Y se deduce que f sería una unidad o de la forma aY, con $a \in \mathbf{k}, a \neq 0$. En el primer

[2]véase la proposición IV.2.6 del libro *Estructuras Algebraicas: Divisibilidad en Anillos Conmutativos*, de J. F. Fernando y J.M. Gamboa.

[3]Hay otros ejemplos, similares a $\mathbf{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, de dominios de ideales principales que no son dominios euclídeos. En este sentido se sabe que $\mathbf{Z}\left[\frac{1+\sqrt{-43}}{2}\right]$, $\mathbf{Z}\left[\frac{1+\sqrt{-67}}{2}\right]$ y $\mathbf{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$ son dominios de ideales principales de ideales principales pero no son dominios euclídeos. Como $\mathbf{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, estos ejemplos son subanillos de $\mathbf{C}$ que contienen a $\mathbf{Z}$ y provienen de la Teoría de Números.

caso, $I = (1)$, lo cual no es posible, ya que (X, Y) ee el conjunto de polinomios de $\mathbf{k}[X, Y]$ con término independiente nulo. En el segundo caso, Y dividiría a X, lo cual también es falso.

Recordemos que $\mathbf{Z}$ y $\mathbf{k}[Y]$ son ambos dominios euclídeos. No es de extrañar entonces que $\mathbf{Z}[X]$ y $\mathbf{k}[X, Y]$ (que igual a $\mathbf{k}[Y][X]$) compartan muchas propiedades; en este caso, el hecho de que ni $\mathbf{Z}[X]$ ni $\mathbf{k}[X, Y]$ sean dominios de ideales principales.

Ya hemos anunciado varias veces que si p es un número primo de $\mathbf{N}$, entonces el ideal (p) de $\mathbf{Z}$ es un ideal maximal. Ha llegado el momento de demostrarlo. Lo haremos como consecuencia de la proposición 3.2.9, que es un resultado más general que se cumple para todo dominio de ideales principales. Antes introducimos un concepto que generaliza la noción de número entero primo en un dominio de integridad cualquiera:

Definición 3.2.6. Sea R un dominio de integridad y sea $p \in R$.

(1) Decimos que p es *irreducible* si $p \neq 0$, $p \notin U(R)$ y para todo $x, y \in R$ tales que $p = xy$, o bien $x \in U(R)$ o bien $y \in U(R)$.

(2) Si $p \neq 0$, $p \notin U(R)$ y p no es irreducible diremos que p es *reducible*.

Ejemplos 3.2.7. (1) Sea $p \in \mathbf{N}$ primo. Entonces p y $-p$ son elementos irreducibles de $\mathbf{Z}$.

(2) Sea $\mathbf{k}$ un cuerpo. Todo polinomio de grado 1 de $\mathbf{k}[X]$ es irreducible, ya que si lo escribimos como producto de dos polinomios, uno de ellos ha de tener necesariamente grado 0, es decir, ha de ser una unidad de $\mathbf{k}[X]$.

(3) La afirmación de (2) no es cierta para polinomios de grado 1 de $R[X]$ si R no es un cuerpo. Por ejemplo, $2X$ es reducible el $\mathbf{Z}[X]$ ya que 2 no es una unidad en $\mathbf{Z}$, por lo que tampoco es una unidad en $\mathbf{Z}[X]$ (¡en cambio $2X$ sí es irreducible en $\mathbf{Q}[X]$!).

(4) El polinomio $X^2 + 1$ es irreducible en $\mathbf{R}[X]$ (en efecto, si fuera reducible, se podría escribir como producto de dos polinomios de $\mathbf{R}[X]$ ambos de grado 1, por lo que $X^2 + 1$ tendría una raíz real y eso es falso). En cambio $X^2 + 1$ es reducible en $\mathbf{C}[X]$, ya que $X^2 + 1 = (X + i)(X - i)$.

Proposición 3.2.8. *Sea R un dominio de integridad y sea $p \in R$, $p \neq 0$. Si el ideal (p) es primo, entonces p es irreducible.*

Demostración. Como (p) es primo, $(p) \neq (1)$, por lo que p no es una unidad. Sean ahora $x, y \in R$ tales que $p = xy$. Entonces $xy \in (p)$ y, como (p) es primo, tenemos que $x \in (p)$ o $y \in (p)$. Entonces, tenemos que $x = x'p$ o $y = y'p$. Si $x = x'p$, entonces $p = xy = x'yp$. Como R es un dominio de integridad y $p \neq 0$, podemos cancelar p en ambos lados de la última igualdad, obteniendo $x'y = 1$, de donde deducimos que y es una unidad de R. Si $y = y'p$, razonando de la misma forma deducimos que x es una unidad de R. □

Proposición 3.2.9. *Sea R un dominio de ideales principales y sea I un ideal no nulo de R. Las siguientes afirmaciones son equivalentes:*

(i) I está generado por un elemento irreducible de R.

(ii) I es primo.

(iii) I es maximal.

En particular, todo ideal primo no nulo de R es maximal.

Demostración. Demostraremos (i) implica (iii), (iii) implica (ii) y (ii) implica (i).

(i) implica (iii): Sea p un elemento irreducible de R. En particular p no es una unidad de R por lo que $(p) \neq (1)$. Sea ahora I un ideal de R tal que $(p) \subset I$. Como R es un dominio de ideales principales, existe $x \in R$ tal que $I = (x)$. Como $p \in (p) \subset I = (x)$, $p = xy$ para algún y de R. Como p es irreducible, o bien x es unidad o bien y es unidad. Si x es unidad, entonces $I = (x) = (1)$. Si y es unidad, entonces $x = y^{-1}p \in (p)$, por lo que $I = (x) \subset (p)$, de donde $I = (p)$.

(iii) implica (ii): Esto es cierto para cualquier anillo por la proposición 2.5.10.

(ii) implica (i): Esto es cierto en cualquier dominio de integridad por la proposición 3.2.8. □

Corolario 3.2.10. *Sea R un dominio de ideales principales y sea $p \in R$. Entonces p es un elemento irreducible si y solo si $R/(p)$ es un cuerpo. En particular, si $p \in \mathbf{N}$, las siguientes afirmaciones son equivalentes:*

(i) p es un número primo;

(ii) (p) es un ideal maximal;

(iii) $\mathbf{Z}/(p)$ es un cuerpo.

Demostración. Por la proposición 3.2.9 un elemento p de un dominio de ideales principales R es irreducible si y solo si (p) es maximal. Por la proposición 2.5.8 esto equivale a que el anillo $R/(p)$ sea un cuerpo. Por otra parte un número natural es primo si y solo si es un elemento irreducible de $\mathbf{Z}$. Como $\mathbf{Z}$ es un dominio de ideales principales, esto equivale a que (p) sea maximal y a que $\mathbf{Z}/(p)$ sea un cuerpo. □

Ejemplo 3.2.11. Aunque ya lo vimos directamente en el ejemplo 3.2.7 (4), damos otra forma de comprobar que $X^2 + 1$ es irreducible en $\mathbf{R}[X]$: vimos en el ejemplo 2.4.6 que $\mathbf{R}[X]/(X^2 + 1)$ es isomorfo a $\mathbf{C}$, por lo que $\mathbf{R}[X]/(X^2 + 1)$ es un cuerpo, así que, según el corolario 3.2.10, el polinomio $X^2 + 1$ es un elemento irreducible de $\mathbf{R}[X]$ (recuerda que $\mathbf{R}[X]$ es un dominio de ideales principales).

Ejemplos 3.2.12. (1) El dominio de integridad $\mathbf{Z}[X]$ no es un dominio de ideales principales ya que posee ideales primos no nulos que no maximales. Por ejemplo, (X) es, según el ejemplo 2.5.5, (3), un ideal primo. Por otra parte, según el ejemplo 2.5.7, (8), (X) no es un ideal maximal. Asimismo, $\mathbf{Z}[X_1, \ldots, X_n]$ no es un dominio de ideales principales.

(2) Si $\mathbf{k}$ es un cuerpo y $n \in \mathbf{N}, n > 1$, entonces $\mathbf{k}[X_1, \ldots, X_n]$ no es dominio de ideales principales ya que posee ideales primos no maximales. Por ejemplo (X_1) es, según el ejemplo 2.5.5, (5), un ideal primo. Por otra parte, según el ejemplo 2.5.9, (3), el ideal (X_1) de $\mathbf{k}[X_1, \ldots, X_n]$ no es maximal.

Vemos a continuación cómo la existencia de una división euclídea con resto único en $\mathbf{Z}$ (en este caso, pidiendo a r, además de la condición (2) de la definición 3.1.4, que sea no negativo) y en $\mathbf{k}[X]$ ($\mathbf{k}$ cuerpo) nos permite dar *representantes distinguidos* para las clases de equivalencia de los anillos cociente de $\mathbf{Z}$ y $\mathbf{k}[X]$.

Proposición 3.2.13. *Sea I un ideal no nulo de $\mathbf{Z}$. Entonces existe $n \in \mathbf{N}$ tal que $I = (n)$ y para todo $\overline{x} \in \mathbf{Z}/I$, existe un único $r \in \mathbf{Z}$, $0 \leq r \leq n-1$ tal que $\overline{x} = \overline{r}$. En particular $\mathbf{Z}/I$ tiene n elementos, que son $\overline{0}, \overline{1}, \ldots, \overline{n-1}$, por lo que podemos elegir $0, 1, \ldots, n-1$ como representantes distinguidos de los elementos de $\mathbf{Z}/I$.*

Demostración. Como $\mathbf{Z}$ es dominio de ideales principales, entonces I está generado por un elemento $m \neq 0$. Si $m > 0$, tomamos $n = m$; si $m < 0$, tomamos $n = -m$. Como -1 es una unidad, en ambos casos $I = (n)$. Dado $\overline{x} \in \mathbf{Z}/I$, por la proposición 3.1.1 existe un (único) elemento r de $\mathbf{Z}$ que cumple $x = nq + r$ y $0 \leq r \leq n-1$. Como $x = nq + r$, entonces $x - r = qn \in (n) = I$, por lo que $x \sim_I r$ y $\overline{x} = \overline{r}$ en $\mathbf{Z}/I$. Por otra parte, si $r' \in \mathbf{Z}$, $0 \leq r' \leq n-1$ y $\overline{x} = \overline{r'}$, entonces $x - r' \in I = (n)$, es decir, existe $q' \in \mathbf{Z}$ tal que $x = nq' + r'$. Entonces $nq + r = x = nq' + r'$ y, por la unicidad del cociente y resto en la proposición 3.1.1, tenemos que $r = r'$. □

Corolario 3.2.14. *Sea $n \in \mathbf{N}$, $n > 1$. El anillo cociente $\mathbf{Z}/(n)$ y el anillo de restos $\mathbf{Z}_n$ (definido en el ejemplo 1.1.19) son isomorfos.*

Demostración. La proposición 3.2.13 nos dice que $\mathbf{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Entonces establecemos la biyección ψ entre $\mathbf{Z}/(n)$ y $\mathbf{Z}_n$ que, para cada $m \in \{0, 1, \ldots, n-1\}$, envía el elemento $\overline{m}$ de $\mathbf{Z}/(n)$ al elemento $\overline{m}$ de $\mathbf{Z}_n$. Vemos que ψ es un homomofismo (por tanto, isomorfismo) de anillos. Si, como nos permite la proposición 3.2.13, trabajamos en $\mathbf{Z}/(n)$ usando representantes distinguidos, la suma y el producto de $\overline{m_1}$ y $\overline{m_2}$ ($0 \leq m_1, m_2 \leq n-1$) es respectivamente $\overline{m_1} + \overline{m_2} = \overline{r}$ y $\overline{m_1} \cdot \overline{m_2} = \overline{s}$, donde r es el resto entre 0 y $n-1$ de dividir $m_1 + m_2$ entre n y s es el resto entre 0 y $n-1$ de dividir $m_1 m_2$ entre n. La suma y el producto en el anillo $\mathbf{Z}_n$ (véase el ejemplo 1.1.19) se definen de la misma manera, una vez que identificamos, usando ψ^{-1}, el elemento $\overline{m}$ de $\mathbf{Z}_n$ con el elemento $\overline{m}$ de $\mathbf{Z}/(n)$. Esto quiere decir que, vía esa identificación, las tablas de la suma y el producto de $\mathbf{Z}/(n)$ y $\mathbf{Z}_n$ son idénticas, por lo que ψ cumple las propiedades (i) y (ii) de la definición 2.3.1. Como

el elemento $\overline{1}$ de $\mathbf{Z}/(n)$ es el elemento neutro del producto en $\mathbf{Z}/(n)$ y el elemento $\overline{1}$ de $\mathbf{Z}_n$ es el elemento neutro del producto en $\mathbf{Z}_n$, la biyección ψ cumple también la propiedad (iii) de la definición 2.3.1. □

Observación 3.2.15. La existencia de un isomorfismo natural ψ justifica la aparente ambigüedad originada por la notación empleada para nombrar los elementos de $\mathbf{Z}/(n)$ y de $\mathbf{Z}_n$.

Corolario 3.2.16. *Sea p un número natural. El anillo de restos $\mathbf{Z}_p$ es un cuerpo si y solo si p es primo.*

Demostración. El resultado es consecuencia de los corolarios 3.2.10 y 3.2.14. □

Ejemplo 3.2.17. Revisamos el ejemplo 2.6.3 a la luz del corolario 3.2.14. Los anillos $\mathbf{Z}_{30}$ y $\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ son isomorfos. El anillo $\mathbf{Z}_{30}$ no es dominio de integridad y tiene 8 unidades. El elemento $\overline{17}$ de $\mathbf{Z}_{30}$ es unidad y su inverso es $\overline{23}$.

Proposición 3.2.18. *Sea $\mathbf{k}$ un cuerpo, sea I un ideal no nulo de $\mathbf{k}[X]$ y sea l el mínimo de los grados de los elementos no nulos de I. Para todo $\overline{f} \in \mathbf{k}[X]/I$ existe un único $r \in \mathbf{k}[X]$ con grado menor que l tal que $\overline{x} = \overline{r}$. Por ello podemos tomar los polinomios de $\mathbf{k}[X]$ de grado menor que l como representantes distinguidos de los elementos de $\mathbf{k}[X]/I$. En particular existe una biyección entre $\mathbf{k}[X]/I$ y el conjunto de polinomios de $\mathbf{k}[X]$ de grado menor que l.*

Demostración. Aunque el argumento es prácticamente el mismo que el de la demostración de la proposición 3.2.13, damos los detalles para mayor claridad. Recordemos que $\mathbf{k}[X]$ es un dominio euclídeo respecto del grado. Por el teorema 3.2.2 existe $g \in \mathbf{k}[X]$ no nulo tal que $I = (g)$ y g tiene grado l. Dado $\overline{f} \in \mathbf{k}[X]/(n)$, por la proposición 3.1.2, existe un (único) elemento r de $\mathbf{k}[X]$ de grado menor que l que cumple $f = gq + r$. Entonces $f - r = qg \in (g) = I$, por lo que $f \sim_I r$ y $\overline{f} = \overline{r}$ en $\mathbf{k}[X]/I$. Por otra parte, si $r' \in \mathbf{k}[X]$, $\overline{f} = \overline{r'}$ y el grado de r' es menor que l, entonces $x - r' \in (g) = I$, es decir, existe $q' \in \mathbf{k}[X]$ tal que $f = gq' + r'$. Entonces $gq + r = f = gq' + r'$ y, por la unicidad del cociente y resto en la proposición 3.1.2, tenemos que $r = r'$. □

Corolario 3.2.19. *Si p es un número primo, I es un ideal no nulo de $\mathbf{Z}_p[X]$ y l es el mínimo de los grados de los elementos no nulos de I, el anillo $\mathbf{Z}_p[X]/I$ tiene p^l elementos.*

Demostración. Por los corolarios 3.2.10 y 3.2.16, el anillo $\mathbf{Z}_p$ es un cuerpo. Por la proposición 3.2.18, hay tantos elementos en $\mathbf{Z}_p[X]/I$ como polinomios de $\mathbf{Z}_p[X]$ de grado menor que l, por lo que $\mathbf{Z}_p[X]/I$ está en biyección con $\mathbf{Z}_p \times \overset{l)}{\cdots} \times \mathbf{Z}_p$. Por otra parte, $\mathbf{Z}_p$ tiene p elementos. □

Observación 3.2.20. Si, como nos permite la proposición 3.2.18, trabajamos en $\mathbf{k}[X]/I$ usando representantes distinguidos, la suma y el producto de $\overline{f_1}$ y $\overline{f_2}$ (los grados de f_1 y f_2 son menores que l, que a su vez es el mínimo de los grados de los elementos no nulos de I) se obtienen como sigue. Sea g un generador de I. Entonces $\overline{f_1} + \overline{f_2} = \overline{r}$ y $\overline{f_1} \cdot \overline{f_2} = \overline{s}$, donde r es el resto de dividir $f_1 + f_2$ entre g y s es el resto de dividir $f_1 f_2$ entre g.

Ejemplo 3.2.21. Revisamos el ejemplo 2.6.5 a la luz de la proposición 3.2.18. Dados $a_1, a_2, \ldots, a_n$ elementos distintos de un cuerpo $\mathbf{k}$ y $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbf{k}$, el ejemplo 2.6.5 y la proposición 3.2.18 nos dicen que existe un único polinomio $p(X)$ de $\mathbf{k}[X]$, de grado menor que n que, para todo $k = 1, 2, \ldots, n$, cumple $p(a_k) = \alpha_k$. El ejemplo 2.6.5 nos dice además cómo calcularlo. [4]

3.3 Dominios de factorización única

Nos fijamos ahora en otra propiedad bien conocida de los números enteros: dado un número entero n, $n \neq 0, 1, -1$, podemos descomponerlo como producto finito de números (naturales) primos o como un producto finito de números (naturales) primos multiplicado por -1 si n es negativo. Además, esta descomposición es única, salvo reordenación de los factores. Esencialmente esta misma propiedad la van a tener dominios de integridad que estudiamos en esta sección, los dominios de factorización única:

Definición 3.3.1. Sea R un dominio de integridad. Decimos que R es un *dominio de factorización única* si, para todo $x \in R$, $x \neq 0$, $x \notin U(R)$

(i) existen $u \in U(R)$, $p_1, \ldots, p_s$ elementos irreducibles no asociados dos a dos (es decir, tales que si $i \neq j$, entonces p_i y p_j no están asociados) y $k_1, \ldots, k_s \in \mathbf{N}$ tales que

$$x = u p_1^{k_1} \cdots p_s^{k_s}; \tag{3.3.1.1}$$

(ii) si existen $v \in U(R)$, $q_1, \ldots, q_t$ elementos irreducibles no asociados dos a dos y $l_1, \ldots, l_t \in \mathbf{N}$ tales que

$$x = v q_1^{l_1} \cdots q_t^{l_t},$$

entonces $s = t$ y, reordenando si es necesario los $q_1, \ldots, q_t$, p_1 y q_1 están asociados, p_2 y q_2 están asociados, $\ldots$, p_s y q_s están asociados y $k_1 = l_1$, $k_2 = l_2$, $\ldots$, $k_s = l_s$.

[4] La existencia de un único polinomio $p(X)$ de $\mathbf{k}[X]$ de grado menor que n se puede demostrar usando solo Álgebra Lineal. También se puede hallar $p(X)$ usando solo Álgebra Lineal. En efecto, los coeficientes de ese polinomio serían la solución del sistema lineal

$$A \cdot \tilde{Y} = \alpha, \tag{3.2.21.1}$$

donde A es la matriz de Van der Monde

$$A = \begin{pmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ \vdots & & & & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{pmatrix},$$

$\tilde{Y} = (Y_0, Y_1, \ldots, Y_{n-1})^t$ y $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)^t$. Como los $a_1, a_2, \ldots, a_n$ son distintos, el determinante de A, que es un producto de factores $(a_i - a_j)$, es no nulo, por lo que el sistema (3.2.21.1) tiene solución única. Lo que aporta de nuevo el ejemplo 2.6.5 es que nos dice cuáles son todos los polinomios que valen α_k en a_k, para cada k, no solo el polinomio $p(X)$ de menor grado.

Observación 3.3.2. La definición 3.3.1 no garantiza la unicidad de la descomposición de x como producto de irreducibles. La razón de que no podamos esperar la unicidad es que si, por ejemplo, p_1 es un elemento irreducible que aparece en (3.3.1.1) y u_1 es una unidad, $p_1' = u_1 p_1$ también es irreducible y $u' = u u_1^{-k_1}$ también es una unidad, por lo que $x = u' p_1'^{k_1} \cdots p_s^{k_s}$ es otra descomposición que cumple (i). Observa que si en el primer párrafo de esta sección parece que en $\mathbf{Z}$ sí tenemos unicidad es porque hemos decidido usar en las descomposiciones elementos irreducibles positivos. Sin embargo, en realidad, en $\mathbf{Z}$ solo tenemos la misma "casi" unicidad de (ii): por ejemplo, $45 = 3^2 \cdot 5 = (-1) \cdot 3^2 \cdot (-5) = (-3)^2 \cdot 5$, etc.

Como decíamos es bien conocido que $\mathbf{Z}$ es un dominio de factorización única; como veremos a continuación, esto va a ocurrir no solo con $\mathbf{Z}$ sino con todos los dominios de ideales principales:

Teorema 3.3.3. *Si R es un dominio de ideales principales, entonces R es un dominio de factorización única.*

Antes de demostrar el teorema 3.3.3 necesitamos varios lemas:

Lema 3.3.4. *Sea R un anillo y sea $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$ una* cadena ascendente *de ideales de R. Entonces $I = \bigcup_{n=1}^{\infty} I_n$ es un ideal de R.*

Demostración. Sean $x, y \in I$. Entonces existen $m, m' \in \mathbf{N}$ tales que $x \in I_m$, $y \in I_{m'}$. Pueden pasar dos cosas, que $m \leq m'$ o que $m' \leq m$. En el primer caso, $x \in I_m \subseteq I_{m'}$ e $y \in I_{m'}$; como $I_{m'}$ es un ideal $x + y \in I_{m'} \subseteq I$. En el segundo caso, razonando de manera análoga llegamos a que $x + y \in I_m \subseteq I$. Sea ahora $a \in R$. Como $x \in I_m$ e I_m es un ideal, $ax \in I_m \subseteq I$. □

Lema 3.3.5. *Sea R un dominio de ideales principales. Toda cadena ascendente $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$ de ideales de R es* estacionaria, *es decir, existe $m \in \mathbf{N}$ tal que $I_m = I_{m+1} = \cdots$.*

Demostración. Sea $I = \bigcup_{n=1}^{\infty} I_n$. Según el lema 3.3.4, I es un ideal. Como R es un dominio de ideales principales, existe $x \in R$ tal que $I = (x)$. Entonces $x \in \bigcup_{n=1}^{\infty} I_n$, por lo que existe $m \in \mathbf{N}$ tal que $x \in I_m$. Veamos ahora $I_{m+k} = I_m$, para todo $k \in \mathbf{N}$. Por hipótesis, $I_m \subseteq I_{m+k}$. Por otro lado $I_{m+k} \subseteq \bigcup_{n=1}^{\infty} I_n = I = (x) \subseteq I_m$. □

Lema 3.3.6. *Sea R un dominio de integridad y sean p, q elementos irreducibles de R. Si p divide a q, entonces p y q están asociados.*

Demostración. Si p divide a q, entonces existe $u \in R$ tal que $q = up$. Como q es irreducible, o u o p son unidades. Como p es irreducible, p no es unidad, por lo que u es unidad. Por la observación 3.1.9, p y q están asociados. □

Demostración del teorema 3.3.3.
Demostración de (i). Sea $x \in R$, $x \neq 0$, $x \notin U(R)$. Vemos primero que x se puede escribir como producto finito de elementos irreducibles de R. Supongamos que no. Entonces,

en particular, x es reducible, por lo que existen $x_1, y_1 \notin U(R)$ tales que $x = x_1y_1$. Además, bien x_1, bien y_1 no puede escribirse como producto finito de elementos irreducibles, pues, en caso contrario, juntando una descomposición finita de x_1 y otra de y_1 obtendríamos una descomposición finita de x, contradiciendo nuestra hipótesis. Renombrando si es necesario x_1 e y_1, podemos suponer que es x_1 el que no se puede escribir como producto finito de irreducibles. Entonces podemos razonar con x_1 como lo hicimos antes con x, por lo que existirán $x_2, y_2 \notin U(R)$ tales que x_2 no se puede escribir como producto finito de irreducibles y $x_1 = x_2y_2$. Podemos seguir este proceso indefinidamente, obteniendo una sucesión de elementos $x_0, x_1, x_2, \ldots, x_n, x_{n+1}, \ldots$ de R, donde $x_0 = x$ y $x_n = x_{n+1}y_{n+1}$, para algún $y_{n+1} \notin U(R)$. Podemos pues construir una cadena ascendente de ideales $(x_0) \subseteq (x_1) \subseteq (x_2) \subseteq \cdots \subseteq (x_n) \subseteq (x_{n+1}) \subseteq \cdots$. Observamos que para todo $n \in \mathbf{N} \cup \{0\}$, $(x_n) \subsetneq (x_{n+1})$. En efecto, si ocurriera $(x_n) = (x_{n+1})$, entonces $x_{n+1} \in (x_n)$, por lo que existiría $z \in R$ tal que $x_{n+1} = zx_n$ y se tendría $x_{n+1} = x_nz = x_{n+1}y_{n+1}z$. Como $x_{n+1} \neq 0$ (si $x_{n+1} = 0$, entonces $x = 0$, lo que contradice nuestra hipótesis inicial sobre x) y R es un dominio de integridad, cancelando x_{n+1} en ambos lados de la igualdad obtendríamos $y_{n+1}z = 1$, por lo que y_{n+1} sería una unidad, pero sabemos por construcción que y_{n+1} no es una unidad. Por tanto hemos construido una cadena ascendente de ideales $(x_0) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots \subsetneq (x_n) \subsetneq (x_{n+1}) \subsetneq \cdots$ no estacionaria. Esto es imposible por el lema 3.3.5. La contradicción viene de suponer que x no se puede escribir como producto finito de irreducibles. Por tanto, todo $x \neq 0$, $x \notin U(R)$ se puede escribir como producto finito de irreducibles.

Consideremos pues una descomposición de x como producto finito de irreducibles, por ejemplo $x = r_1 \cdots r_m$, donde $r_1, \ldots, r_m$ son irreducibles. Según el ejercicio 3.1.10, "estar asociado a" es una relación de equivalencia en $R \setminus \{0\}$ y, de hecho, también lo es en cualquier subconjunto de R, por ejemplo, en $\{r_1, \ldots, r_m\}$. Agrupamos los $r_1, \ldots, r_m$ en clases de equivalencia de manera que la clase de, por ejemplo, r_1, esté formada por todos aquellos elementos de $\{r_1, \ldots, r_m\}$ que están asociados a r_1. Renombrando si es necesario los $r_1, \ldots, r_m$, podemos suponer que la clase de equivalencia de r_1 está formada por $r_1, \ldots, r_{k_1}$, donde $1 \leq k_1 \leq m$. Por la observación 3.1.9, existen $w_2, \ldots, w_{k_1} \in U(R)$ tales que $r_2 = w_2r_1, \ldots, r_{k_1} = w_{k_1}r_1$. Llamamos $p_1 = r_1$ y $u_1 = w_2 \cdots w_{k_1}$, que es una unidad de R, de forma que $r_1 \cdots r_{k_1} = u_1p_1^{k_1}$. Si $k_1 < m$, razonamos de igual manera para r_{k_1+1} y, llamando $p_2 = r_{k_1+1}$, vemos que existen $u_2 \in U(R)$ y $1 \leq k_2 \leq m - k_1$ tales que $r_{k_1+1} \cdots r_{k_1+k_2} = u_2p_2^{k_2}$. Seguimos el proceso hasta acabar con todos los elementos de $\{r_1 \cdots r_m\}$, obteniendo elementos irreducibles $p_1, \ldots, p_s$, números naturales $k_1, \ldots, k_s$ y unidades $u_1, \ldots, u_s$ tales que

$$x = up_1^{k_1} \cdots p_s^{k_s}, \tag{3.3.6.1}$$

donde $u = u_1 \cdots u_s$ es también una unidad. Observamos finalmente que si $i \neq j$, entonces p_i y p_j pertenecen a clases de equivalencia distintas en el conjunto $\{r_1 \cdots r_m\}$, por lo que p_i y p_j no están asociados. Por tanto (3.3.6.1) cumple lo pedido en el apartado (i) del enunciado del teorema 3.3.3.

Demostración de (ii). Sea $x \in R$, $x \neq 0$, $x \notin U(R)$ y sean por una parte $u \in U(R)$, $p_1, \ldots, p_s$

elementos irreducibles no asociados dos a dos y $k_1, \ldots, k_s \in \mathbf{N}$ y, por otra parte, $v \in U(R)$, $q_1, \ldots, q_t$ elementos irreducibles no asociados dos a dos y $l_1, \ldots, l_t \in \mathbf{N}$ tales que

$$x = up_1^{k_1} \cdots p_s^{k_s} = vq_1^{l_1} \cdots q_s^{l_t}. \tag{3.3.6.2}$$

Vemos primero que $s = t$. Sea $p_i \in \{p_1, \ldots, p_s\}$. Como R es un dominio de ideales principales y p_i es irreducible, según la proposición 3.2.9, el ideal (p_i) es primo. Por (3.3.6.2), $vq_1^{l_1} \cdots q_s^{l_t} \in (p_i)$. Como $v \in U(R)$, $v \notin (p_i)$, pues de otra forma $(p_i) = (1)$. Por tanto, al ser (p_i) primo, $q_1^{l_1} \cdots q_s^{l_t} \in (p_i)$. Si $q_1 \in (p_i)$, entonces p_i divide a q_1 y, como p_i, q_1 son irreducibles, q_1 divide a p_i y p_i y q_1 están asociados por el lema 3.3.6. Si $q_1 \notin (p_i)$, entonces $q_1^{l_1} \notin (p_i)$ al ser (p_i) primo, por lo que $q_2^{l_2} \cdots q_s^{l_t} \in (p_i)$. Repetimos el razonamiento que hemos hecho para q_1 con $q_2, q_3, \ldots$ cuantas veces sea necesario hasta encontrar $q_j \in \{q_1, \ldots, q_t\}$ asociado a p_i. Por otra parte, no existe otro elemento de $\{q_1, \ldots, q_t\}$ asociado a p_i más que q_j. En efecto, supongamos que existiera $q_{j'}$ asociado a p_i. Como "estar asociado a" es una relación de equivalencia en $\{p_1, \ldots, p_s, q_1, \ldots, q_t\}$, en ese caso, por la propiedad transitiva de dicha relación, q_j y $q_{j'}$ estarían asociados. Comos los elementos de $\{q_1, \ldots, q_t\}$ son no asociados dos a dos, se tiene $j = j'$. Todo esto nos permite definir la aplicación

$$\begin{array}{rccc} \phi: & \{p_1, \ldots, p_s\} & \longrightarrow & \{q_1, \ldots, q_t\} \\ & p_i & \mapsto & q_j \end{array}$$

donde q_j es el único elemento de $\{q_1, \ldots, q_t\}$ asociado a p_i (el que exista un único elemento de $\{q_1, \ldots, q_t\}$ asociado a p_i es lo que hace que ϕ esté bien definida). Por otro lado, ϕ es inyectiva, ya que si p_i y $p_{i'}$ están asociados a q_j, de nuevo por la propiedad transitiva de la relación "estar asociado a", p_i y $p_{i'}$ están asociados, por lo que $i = i'$. Como $\{p_1, \ldots, p_s\}$ y $\{q_1, \ldots, q_t\}$ son conjuntos finitos y ϕ es una aplicación inyectiva, el cardinal de $\{p_1, \ldots, p_s\}$, que es s, es menor o igual que el cardinal de $\{q_1, \ldots, q_t\}$, que es t. Intercambiando en todo el razonamiento anterior los papeles de $\{p_1, \ldots, p_s\}$ y $\{q_1, \ldots, q_t\}$, podemos construir una aplicación inyectiva de $\{q_1, \ldots, q_t\}$ a $\{p_1, \ldots, p_s\}$ (que será, a posteriori, inversa de ϕ), de lo que concluimos que $t \leq s$, por lo que $s = t$.

Como $\{p_1, \ldots, p_s\}$ y $\{q_1, \ldots, q_s\}$ son conjuntos finitos con el mismo cardinal y ϕ es inyectiva, concluimos que ϕ es biyectiva, por lo que nos permite emparejar cada elemento de $\{p_1, \ldots, p_s\}$ con un elemento de $\{q_1, \ldots, q_s\}$, por lo que, renombrando los $q_1, \ldots, q_s$ si es necesario, podemos suponer que p_1 está asociado a q_1, p_2 a q_2, $\ldots$, p_s a q_s.

Vemos por último que $k_1 = l_1, k_2 = l_2, \ldots, k_s = l_s$. Hacemos el razonamiento para k_1 y l_1, siendo el razonamiento para los demás casos análogo. Sea $v_1 \in U(R)$ tal que $q_1 = v_1 p_1$. Supongamos que $k_1 \neq l_1$. Entonces $k_1 < l_1$ o $k_1 > l_1$. En el primer caso, en la expresión

$$up_1^{k_1} \cdots p_s^{k_s} = vq_1^{l_1} \cdots q_s^{l_t}$$

podemos cancelar $p_1^{k_1}$ en ambos lados, ya que R es un dominio de integridad y $p_1 \neq 0$. Nos queda entonces

$$up_2^{k_2} \cdots p_s^{k_s} = vv_1^{l_1} p_1^{l_1 - k_1} q_2^{l_2} \cdots q_s^{l_t}.$$

Como $l_1 > k_1$, se sigue $l_1 - k_1 > 0$ y tenemos dos descomposiciones como productos de irreducibles de un mismo elemento de R y ambas descomposiciones cumplen (i) de la definición 3.3.1. Sin embargo la descomposición de la izquierda tiene $s-1$ irreducibles no asociados mientras que la descomposición de la derecha tiene s irreducibles no asociados. Esto contradice lo que hemos probado más arriba. Por tanto no puede ocurrir $k_1 < l_1$ y, realizando un razonamiento simétrico, vemos que tampoco puede ocurrir $k_1 > l_1$, por lo que $k_1 = l_1$. □

Corolario 3.3.7. *Los anillos* $\mathbf{Z}$, $\mathbf{k}[X]$ *(*$\mathbf{k}$ *cuerpo),* $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$ *y* $\mathbf{Z}[\sqrt{-2}]$ *son dominios de factorización única.*

Demostración. Todos los anillos que aparecen en el enunciado del corolario son dominios euclídeos, por lo que, por el teorema 3.2.2, son dominios de ideales principales. Estos a su vez son dominios de factorización única por el teorema 3.3.3. □

Proposición 3.3.8. *(Lema de Euclídes). Sea R un dominio de factorización única, sea $p \in R$ irreducible y sean $x, y \in R$. Si p divide a xy, entonces p divide a x o p divide a y.*

Demostración. Si x o y son nulos, el resultado es trivial, así que suponemos $x, y \neq 0$. Sea $z \in R$ tal que $xy = zp$. No puede ocurrir que x e y sean ambos unidades, pues en ese caso xy es unidad y p también lo sería, lo cual es imposible, ya que p es irreducible por hipótesis. Entonces, o bien x es una unidad, o bien y es una unidad, o bien ni x ni y son unidades. En el primer caso tenemos que $y = x^{-1}zp$, por lo que p divide a y. En el segundo caso, razonando de forma análoga concluimos que p divide a x. En el tercer caso, sean

$$x = up_1^{k_1} \cdots p_s^{k_s}, \quad y = vq_1^{l_1} \cdots q_s^{l_t}, \quad z = wr_1^{m_1} \cdots r_h^{m_h}$$

descomposiciones de x, y, z como producto de irreducibles que cumplen (i) de la definición 3.3.1. Tenemos pues

$$xy = (uv)p_1^{k_1} \cdots p_s^{k_s} q_1^{l_1} \cdots q_s^{l_t} \quad \text{y} \quad xy = pz = wpr_1^{m_1} \cdots r_h^{m_h}$$

dos descomposiciones de xy como producto de irreducibles. Por (ii) de la definición 3.3.1, p debe estar asociado a algún p_i o a algún q_j. En el primer caso p divide a x y en el segundo caso p divide a y. □

Observación 3.3.9. La propiedad de que si p divide a xy, entonces p divide a x o p divide a y es equivalente a que (p) sea un ideal primo. Por eso, a los elementos de R que cumplen esa propiedad se les llama elementos *primos*.

Corolario 3.3.10. *Sea R un dominio de factorización única y sea $p \in R$. Las siguientes afirmaciones son equivalentes:*

(i) el elemento p es irreducible;

(ii) el elemento p es primo;

(iii) el ideal (p) es primo.

Demostración. La proposición 3.3.8 dice que (i) implica (ii). Las afirmaciones (ii) y (iii) son equivalentes según dijimos en la observación 3.3.9. La proposición 3.2.8 nos dice que (iii) implica (i) en cualquier dominio de integridad. □

El corolario 3.3.10 nos permite dar la siguiente caracterización de los dominios de factorización única, que, de hecho, se puede tomar como definición alternativa de los mismos:

Corolario 3.3.11. *Un dominio de integridad R es un dominio de factorización única si y solo si R cumple las siguientes propiedades:*

(i') Todo elemento no nulo de R que no sea unidad se puede escribir como producto finito de elementos irreducibles.

(ii') Todo elemento irreducible de R es primo.

Demostración. Si R es un dominio de factorización única, entonces la propiedad (i) de la definición 3.3.1 implica la propiedad (i') del enunciado. Por otra parte, la propiedad (ii') del enunciado se sigue del corolario 3.3.10.

Supongamos ahora que R es un dominio de integridad que cumple (i') y (ii'). Vimos en la demostración del teorema 3.3.3 que la propiedad (i') del enunciado implica la propiedad (i) de la definición 3.3.1. En esa misma demostración vimos también que, para demostrar la propiedad (ii) de la definición 3.3.1 solo usábamos el hecho de que, en un dominio de ideales principales, todo elemento irreducible es primo (esto se sigue de la proposición 3.2.9). En este caso R no es necesariamente un dominio de ideales principales pero cumple que todo irreducible es primo por la hipótesis (ii'). □

Ejemplos 3.3.12. Veremos en el tema siguiente que si R es un dominio de factorización única, entonces $R[X]$ también es un dominio de factorización única (teorema 4.4.2). De ello se deduce que, si $\mathbf{k}$ es un cuerpo, $\mathbf{k}[X_1, \ldots, X_n]$ es un dominio de factorización única (corolario 4.4.3). Asimismo $\mathbf{Z}[X_1, \ldots, X_n]$ es un dominio de factorización única (corolario 4.4.3).

Sin embargo, como vimos en los ejemplos 3.2.5 y 3.2.12, $\mathbf{k}[X_1, \ldots, X_n]$ no es un dominio de ideales principales si $n \geq 2$ y $\mathbf{Z}[X_1, \ldots, X_n]$ tampoco es un dominio de ideales principales.

Observación 3.3.13. Los subanillos $\mathbf{Z}[\sqrt{-3}]$ y $\mathbf{Z}[\sqrt{10}]$ de $\mathbf{C}$ son dominios de integridad pero no son dominios de factorización única (véanse los ejercicios 9 y 10 de la hoja 3).

Observación 3.3.14. Los teoremas 3.2.2 y 3.3.3, los ejemplos 3.2.3, (2) y 3.3.12 y la observación 3.3.13 muestran que existe la siguiente jerarquía entre las diferentes clases de dominios:

$$\begin{array}{ccccccc} \text{D.E.} & \Rightarrow & \text{D.I.P.} & \Rightarrow & \text{D.F.U.} & \Rightarrow & \text{D.I.} \\ & \not\Leftarrow & & \not\Leftarrow & & \not\Leftarrow & \end{array}$$

3.4 Máximo común divisor

Definición 3.4.1. Sea R dominio de integridad y sean $x, y \neq 0$. Decimos que $z \in R$ es un *máximo común divisor* de x e y si

(i) z es un *divisor común* de x e y, es decir, z divide a x y z divide a y;

(ii) para todo $z' \in R$ tal que z' divide a x y a y, z' divide también a z.

Proposición 3.4.2. *Si z_1 es un máximo común divisor de x e y, entonces z_2 es un máximo común divisor de x e y si y solo si z_2 está asociado a z_1. En particular, si existe un máximo común divisor de x e y, este es único salvo producto por una unidad.*

Demostración. En efecto, sean z_1 y z_2 máximos comunes divisores de x e y. Por (i), z_2 es un divisor común de x e y y por (ii), al ser z_1 un máximo común divisor de x e y, z_2 divide a z_1. Intercambiando los papeles de z_1 y z_2 en el argumento anterior vemos que z_1 divide a z_2, por lo que z_1 y z_2 están asociados. Por otra parte, si z_1 es un máximo común divisor de x e y y z_2 está asociado a z_1, entonces z_2 divide a z_1, por lo que también divide a x y a y. Sea ahora z' un divisor común a x y a y. Como z_1 es un máximo común divisor de x e y, z' divide a z_1 y, como z_1 y z_2 están asociados, z_1 divide a z_2, por lo que z' divide a z_2. □

Al igual que ocurre en $\mathbf{Z}$, en todo dominio de factorización única existe máximo común divisor:

Proposición 3.4.3. *Sea R un dominio de factorización única y sean $x, y \in R$, $x, y \neq 0$. Si $x, y \notin U(R)$,*

(i) sean $x = up_1^{k_1} \cdots p^{k_s}$ e $y = vq_1^{l_1} \cdots q^{l_s}$ descomposiciones de x e y como producto de irreducibles que cumplen (i) de la definición 3.3.1;

(ii) sea $i \in \mathbf{N} \cup \{0\}$ tal que p_1 está asociado a q_1, p_2 está asociado a q_2, ..., p_i está asociado a q_i y ninguno de los $p_{i+1}, \ldots, p_s$ está asociado a ninguno de los $q_{i+1}, \ldots, q_t$; y

(iii) sean $m_1 = mín(k_1, l_1), \ldots, m_i = mín(k_i, l_i)$.

En ese caso

(a) si x o y es una unidad, entonces 1 es un máximo común divisor de x e y;

(b) si $x, y \notin U(R)$ e $i = 0$, entonces 1 es un máximo común divisor de x e y;

(c) si $x, y \notin U(R)$ e $i > 0$, entonces $p_1^{m_1} \cdots p_i^{m_i}$ es un máximo común divisor de x e y.

Demostración. Dejamos la prueba de esta proposición como ejercicio. □

Identidad de Bézout:

Proposición 3.4.4. *Sea R un dominio de integridad y sean $x, y \in R$, $x, y \neq 0$. Si $z \in R$ es tal que $(x, y) = (z)$, entonces z es un máximo común divisor de x e y.*

Demostración. Si $(x, y) = (z)$, entonces $x \in (z)$ e $y \in (z)$, por lo que z divide a x y z divide a y. Sea ahora z' que divide a x y a y. Existen $a', b' \in R$ tales que $x = a'z'$, $y = b'z'$. Como $z \in (x, y)$, existen $a, b \in R$ tales que $z = ax + by$, de donde $z = ax + by = aa'z' + bb'z' = (aa' + bb')z'$, por lo que z' divide a z. □

Proposición 3.4.5. *Sea R un dominio de ideales principales y sean $x, y \in R, x, y \neq 0$. Entonces z es un máximo común divisor de x e y si y solo si $(z) = (x, y)$.*

Demostración. Si $(z) = (x, y)$, la proposición 3.4.4 nos dice que z es un máximo común divisor de x e y. Sea ahora z un máximo común divisor de x e y. Como R es un dominio de ideales principales, existe $\hat{z} \in R$ tal que $(\hat{z}) = (x, y)$. De nuevo según la proposición 3.4.4, $\hat{z}$ es un máximo común divisor de x e y. Según la proposición 3.4.2, z y $\hat{z}$ están asociados, por lo que $(z) = (\hat{z}) = (x, y)$. □

Ejemplos 3.4.6. (1) En $\mathbf{Z}$, $(12, 28) = (4)$ y $(2, 5) = (1)$ y, en efecto, 4 es máximo común divisor de 12 y 28 y 1 es máximo común divisor de 2 y 5.

(2) En $\mathbf{R}[X]$, 1 se puede escribir como $X^2 + 1 + (-X)X$, por lo que $(1) = (X^2 + 1, X)$. Por tanto 1 es máximo común divisor de $X^2 + 1$ y X.

(3) Usamos las propiedades del máximo común divisor para ver que el ideal (X, Y) de $\mathbf{R}[X, Y]$ no es principal. Los elementos X e Y son irreducibles no asociados de $\mathbf{R}[X, Y]$ por lo que 1 es un máximo común divisor de X e Y. Si existiera $f \in \mathbf{R}[X, Y]$ tal que $(X, Y) = (f)$, entonces f sería un máximo común divisor de X e Y, por lo que estaría asociado a 1 y sería una unidad. En ese caso $(X, Y) = (1)$, lo cual es falso.

Corolario 3.4.7. *(Identidad de Bézout). Sea R un dominio de ideales principales y sean $x, y \in R, x, y \neq 0$.*

(1) Si z es máximo común divisor de x e y, entonces existen $a, b \in R$ tales que $z = ax + by$ (a y b reciben el nombre de coeficientes de Bézout *para la terna (x, y, z)).*

(2) Los elementos x e y son primos entre sí *(es decir, 1 es máximo común divisor de x e y) si y solo si existen $a, b \in R$ tales que $1 = ax + by$.*

Demostración. La afirmación (1) y una de las implicaciones de (2) son consecuencias inmediatas de la proposición 3.4.5. Para la otra implicación de (2), si existen $a, b \in R$ tales que $1 = ax + by$, entonces $(1) \subset (x, y)$, por lo que $(1) = (x, y)$. En ese caso, 1 es máximo común divisor de x e y por la proposición 3.4.5. □

Observación 3.4.8. La identidad de Bézout no tiene por qué cumplirse en dominios de factorización única que no son dominios de ideales principales. Por ejemplo, en $\mathbf{R}[X, Y]$, 1 es máximo común divisor de X e Y, pero no es posible escribir 1 como combinación de X e Y con coeficientes en $\mathbf{R}[X, Y]$, pues (X, Y) es distinto de (1).

Corolario 3.4.9. *Sea R un dominio de ideales principales, sea I un ideal de R, no nulo y distinto de* (1)*, sea x un generador de I y sea $y \in I$.*

(1) El elemento $\overline{y}$ de R/I es una unidad de R/I si y solo si x e y son primos entre sí.

(2) Si x e y son primos entre sí y a y b son coeficientes de Bézout para $(x, y, 1)$ (es decir, $1 = ax + by$), entonces $\overline{b}$ es el inverso de $\overline{y}$ en R/I.

Demostración. Sea $y \in R$ y consideremos $\overline{y}$ en R/I. Entonces $\overline{y}$ es una unidad de R/I si y solo si existe $b \in R$ tal que $\overline{y} \cdot \overline{b} = \overline{1}$ en R/I. Esto equivale a que $\overline{yb} = \overline{1}$ en R/I. Esto equivale a que $1 - yb \in I$. Esto equivale a que exista $a \in R$ tal que $1 - yb = ax$. Esto equvale a que existan $a, b \in R$ tales que $1 = ax + by$ y a que, por el corolario 3.4.7, x e y sean primos entre sí. □

Corolario 3.4.10. *Sean m y n dos enteros primos entre sí. Entonces la aplicación*

$$\begin{array}{rccc} \overline{\varphi}: & \dfrac{\mathbf{Z}}{(mn)} & \longrightarrow & \dfrac{\mathbf{Z}}{(m)} \times \dfrac{\mathbf{Z}}{(n)} \\ & x + (mn) & \mapsto & (x + (m), x + (n)) \end{array}$$

está bien definida y es un isomorfismo de anillos.

Demostración. Por el ejercicio 2 (a) del tema 2, $(m)(n) = (mn)$. Como 1 es máximo común divisor de m y n, por la proposición 3.4.5, $(1) = (m, n) = (m) + (n)$, es decir, los ideales (m) y (n) son coprimos. Entonces por el teorema 2.6.1 (el teorema chino del resto), la aplicación $\overline{\varphi}$ está bien definida y es un isomorfismo de anillos. □

Corolario 3.4.11. *Sean $m_1, m_2, \ldots, m_k$ números enteros, primos entre sí dos a dos (es decir, si $i \neq j$, entonces m_i y m_j son primos entre sí) y sea $m = m_1 m_2 \cdots m_k$. La aplicación*

$$\begin{array}{ccc} \dfrac{\mathbf{Z}}{(m)} & \longrightarrow & \dfrac{\mathbf{Z}}{(m_1)} \times \cdots \times \dfrac{\mathbf{Z}}{(m_k)} \\ x + (m) & \mapsto & (x + (m_1), \ldots, x + (m_k)) \end{array}$$

está bien definida y es un isomorfismo de anillos.

Demostración. Para todo $1 < i \leq k$, los números m_i y $m_1 \cdots m_{i-1}$ son primos entre sí, ya que ninguno de los irreducibles que dividen a m_i divide a ninguno de los números $m_1, \ldots, m_{i-1}$. La demostración se hace entonces por inducción en k, usando el corolario 3.4.10 y la observación de que, para todo $1 < i \leq k$, la aplicación

$$\begin{array}{rccc} \overline{\varphi}_i: & \dfrac{\mathbf{Z}}{(m_1 \cdots m_i)} & \longrightarrow & \dfrac{\mathbf{Z}}{(m_1)} \times \cdots \times \dfrac{\mathbf{Z}}{(m_i)} \\ & x + (m) & \mapsto & (x + (m_1), \ldots, x + (m_i)) \end{array}$$

es $\overline{\varphi}_i = (\overline{\varphi}_{i-1} \times \iota_i) \circ \overline{\psi}_i$, donde ι_i es la identidad en $\mathbf{Z}/(m_i)$ y

$$\begin{array}{rccc} \overline{\psi}_i : & \dfrac{\mathbf{Z}}{(m_1 \cdots m_i)} & \longrightarrow & \dfrac{\mathbf{Z}}{(m_1 \cdots m_{i-1})} \times \dfrac{\mathbf{Z}}{(m_i)} \\ & x + (m_1 \cdots m_i) & \mapsto & (x + (m_1 \cdots m_{i-1}), x + (m_i)). \end{array}$$

□

Ejemplo 3.4.12. Como ejemplo del corolario 3.4.11 tenemos el ejemplo 2.6.3. En aquella ocasión vimos de manera explícita que los ideales (2) y (3) son coprimos y tambíen los ideales (6) y (5). Así, si usando la notación del corolario 3.4.11, llamamos $m_1 = 2, m_2 = 3$ y $m_3 = 5$, vimos directamente que $\overline{\varphi}_2$ y $\overline{\psi}_3$ son isomorfismos de anillos.

Algoritmo de Euclides:

Sea R un dominio de factorización única. Factorizar un elemento x de R como producto de irreducibles es, en general, muy complicado, incluso si $R = \mathbf{Z}$ (piensa en el caso de que x sea un número natural muy grande). Por ello, la forma de calcular el máximo común divisor sugerida en la proposición 3.4.3 es poco eficaz. Afortunadamente, si R es un dominio euclídeo, tenemos un algoritmo, el *algoritmo de Euclides*, que nos permite calcular el máximo común divisor de dos elementos de manera más sencilla.

Proposición 3.4.13. *Sea R un dominio euclídeo y sean $x, y \in R, x, y \neq 0$. Definimos r_1 como el resto de dividir x entre y; si $r_1 \neq 0$, definimos r_2 como el resto de dividir el elemento y entre r_1; si $r_2 \neq 0$, definimos r_3 como el resto de dividir r_1 entre r_2, etc. Entonces*

(1) existe $n \in \mathbf{N}$ tal que el resto de dividir r_{n-1} entre r_n es 0;

(2) r_n es máximo común divisor de x e y.

Demostración. La afirmación (1) se cumple porque si no tendríamos una sucesión infinita $\{y, r_1, r_2, \ldots, r_m, \ldots\}$ de elementos de R que daría lugar a una sucesión infinita $\delta(y) > \delta(r_1) > \delta(r_2) > \cdots > \delta(r_m) > \cdots$ de elementos de $\mathbf{N} \cup \{0\}$ estrictamente decreciente, lo cual es imposible.

Por tanto tenemos las siguientes igualdades:

$$\begin{array}{ccccc} x & = & yq_1 & + & r_1 \\ y & = & r_1q_2 & + & r_2 \\ r_1 & = & r_2q_3 & + & r_3 \\ \vdots & & \vdots & & \vdots \\ r_{n-2} & = & r_{n-1}q_n & + & r_n \\ r_{n-1} & = & r_nq_{n+1}. & & \end{array}$$

Recordemos que si c divide a a y b, entonces c divide a $a + b$. Entonces, por la última igualdad, r_n divide a r_{n-1}. Por la penúltima igualdad r_n divide a r_{n-2} y, siguiendo el

razonamiento, r_n divide a $r_{n-1}, \ldots, r_2, r_1$. La segunda igualdad nos dice entonces que r_n también divide a y. Finalmente, como r_n divide a r_1 y a y, la primera igualdad nos dice que r_n divide también a x. Por tanto, r_n es un divisor común de x e y.

Sea ahora z' otro divisor común de x e y. La primera igualdad nos dice que z' divide a r_1. La segunda igualdad nos dice que z' divide a r_2, etc., por lo que, finalmente, la penúltima igualdad nos dice que z' divide a r_n. □

Ejemplo 3.4.14. Calculamos el máximo común divisor de 35 y 27 y los coeficientes de la identidad de Bézout usando el algoritmo de Euclídes:

$$\begin{array}{rcl} 35 & = & 27 \cdot 1 + 8 \\ 27 & = & 8 \cdot 3 + 3 \\ 8 & = & 3 \cdot 2 + 2 \\ 3 & = & 2 \cdot 1 + 1 \\ 2 & = & 1 \cdot 2 \end{array}$$

por tanto 1 es máximo común divisor de 35 y 27.

Por otra parte, de las igualdades anteriores deducimos:
$1 = 3 - 2$ y $2 = 8 - 2 \cdot 3$, de donde $1 = 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8$;
$3 = 27 - 3 \cdot 8$, de donde $1 = 3(27 - 3 \cdot 8) - 8 = 3 \cdot 27 + (-10) \cdot 8$;
$8 = 35 - 27$, de donde $1 = 3 \cdot 27 - 10(35 - 27)$ y

$$1 = (-10) \cdot 35 + 13 \cdot 27. \tag{3.4.14.1}$$

Ejemplo 3.4.15. Como 27 y 35 son primos entre sí, según el corolario 3.4.9 (1), $\overline{27}$ es una unidad en $\mathbf{Z}/(35)$. Como -10 y 13 son coeficientes de Bezout, según hemos visto en (3.4.14.1), el corolario 3.4.9 (2) nos dice que el inverso de $\overline{27}$ en $\mathbf{Z}/(35)$ es $\overline{13}$. En efecto, como $1 = (-10)\cdot 35 + 13 \cdot 27$, tomando clases en $\mathbf{Z}/(35)$ tenemos $\overline{1} = -\overline{10}\cdot\overline{35} + \overline{13}\cdot\overline{27} = \overline{13}\cdot\overline{27}$.

Observación 3.4.16. Los ejemplos 3.4.14 y 3.4.15 nos muestran cómo podemos calcular, usando el corolario 3.4.9 y el algoritmo de Euclides, el inverso de una unidad en los anillos $\mathbf{Z}_n$, $\mathbf{Z}/(n)$, en los anillos cociente de $\mathbf{k}[X]$ ($\mathbf{k}$ cuerpo) y, en general, en los anillos cociente de un dominio euclídeo.

Ejemplo 3.4.17. La observación 2.6.2 nos da el inverso del isomorfismo $\overline{\varphi}$ del corolario 3.4.10. El algoritmo de Euclides nos permite calcular dicho inverso. Lo vemos para el isomorfismo

$$\begin{array}{rccc} \overline{\varphi}: & \dfrac{\mathbf{Z}}{(945)} & \longrightarrow & \dfrac{\mathbf{Z}}{(27)} \times \dfrac{\mathbf{Z}}{(35)} \\ & x + (945) & \mapsto & (x + (27), x + (35)), \end{array} \tag{3.4.17.1}$$

$(945 = 27 \cdot 35)$. Por ejemplo, hallamos el inverso por $\overline{\varphi}$ del elemento $(5 + (27), 8 + (35))$. Según (3.4.14.1),

$$1 = 13 \cdot 27 + (-10) \cdot 35 = 351 + (-350),$$

donde $351 \in (27)$ y $-350 \in (35)$. Entonces, según la observación 2.6.2, el inverso de $(5 + (27), 8 + (35)$ será $1050 + (945) = 105 + (945)$, ya que $5(-350) + 8 \cdot 351$. En general, el inverso por $\overline{\varphi}$ de $(y + (27), z + (35))$ es $x + (945)$, donde $x = -350y + 351z$.

Ecuaciones diofánticas lineales:

Definición 3.4.18. Una *ecuación diofántica lineal* en dos incógnitas X e Y es una expresión

$$aX + bY = c, \tag{3.4.18.1}$$

donde a, b y c son enteros. Una solución de la ecuación diofántica (3.4.20.1) es un par (α, β) de enteros tales que $a\alpha + b\beta = c$ (es decir, cuando resolvemos una ecuación diofántica buscamos solo las soluciones enteras de la ecuación).

El siguiente corolario del corolario 3.4.7 sirve, entre otras cosas, para decidir si una ecuación diofántica tiene solución.

Corolario 3.4.19. *Sea R un dominio de ideales principales, sean $a, b, c \in R, a, b, c \neq 0$. Existen $x, y \in R$ tales que $ax + by = c$ si y solo si el máximo común divisor de a e b divide a c.*

Demostración. Sea d el máximo común divisor de a e b. Supongamos que existan $x, y \in R$ tales que $ax + by = c$. Como d divide a a y a b, entonces divide también a c. Supongamos ahora que $c = td$, para algún $t \in R$. Por el corolario 3.4.7 (1), existen $x', y' \in R$ tales que $d = x'a + y'b$, de donde $c = td = a(tx) + b(ty)$. □

Ejemplo 3.4.20. Consideremos la ecuación diofántica

$$27X + 35Y = 3. \tag{3.4.20.1}$$

Como 1 es máximo común divisor de 27 y 35 y, obviamente, 1 divide a 3, según el corolario 3.4.19, la ecuación diofántica (3.4.20.1) tiene solución (entera). Vamos a calcular ahora todas las soluciones (enteras) de (3.4.20.1). Hallamos primero una solución particular. Multiplicando (3.4.14.1) por 3 vemos que $X = 39, Y = -30$ es una solución de (3.4.20.1). Por otra parte, (3.4.20.1) es la ecuación de una recta L en el plano afín $\mathbf{R}^2$, cuyos puntos obtenemos escribiendo unas ecuaciones paramétricas de L, como por ejemplo

$$\begin{aligned} X &= 39 - 35\lambda \\ Y &= -30 + 27\lambda \end{aligned} \tag{3.4.20.2}$$

Entonces las soluciones de la ecuación diofántica (3.4.20.1) son los puntos L con ambas coordenadas enteras. Como $39, -35, -30$ y 27 son números enteros, si tomamos λ en $\mathbf{Z}$, el par $(39 - 35\lambda, -30 + 27\lambda)$ tiene ambas coordenadas enteras. Por otra parte, si (x, y) es una solución (entera) de (3.4.20.1), el valor correspondiente de λ para el punto (x, y) es $\lambda = \frac{x - 39}{-35} = \frac{y + 30}{27}$, que es un número racional. Sean entonces λ_1 y λ_2 enteros no nulos y primos entre sí tales que $\lambda = \frac{\lambda_1}{\lambda_2}$. Como $-35\lambda = x - 39$ y $27\lambda = y + 30$, tenemos que $-35\lambda, 27\lambda \in \mathbf{Z}$. Como λ_1 y λ_2 son primos entre sí, por el lema de Euclides, λ_2 divide a -35 y a 27. Como -35 y 27 son primos entre sí, $\lambda_2 = \pm 1$, por lo que $\lambda \in \mathbf{Z}$. Por tanto el conjunto de soluciones (enteras) de la ecuación diofántica (3.4.20.1) es $\{(39 - 35\lambda, -30 + 27\lambda) \mid \lambda \in \mathbf{Z}\}$.

3.5 Sistemas de congruencias

Definición 3.5.1. Sea $m \in \mathbf{N}$. Decimos que dos números enteros a y b son *congruentes módulo* m y escribimos $a \equiv b\,(m)$ o $a \equiv b$ mód m si m divide a $a - b$.

Observación 3.5.2. La relación de congruencia es la relación de equivalencia inducida en $\mathbf{Z}$ por el ideal (m). Por tanto, las siguientes afirmaciones son equivalentes:

(1) $a \equiv b$ mód m;

(2) a y b tienen el mismo resto, entre 0 y $m-1$, al dividirlos por m;

(3) $\overline{a} = \overline{b}$ en $\mathbf{Z}/(m)$.

Ejemplo 3.5.3. Vamos hallar la solución de la *congruencia*

$$x \equiv 3 \text{ mód } 41,$$

es decir, vamos a hallar todos los x de $\mathbf{Z}$ tales que x es congruente con 3 módulo 41. Serán aquellos x de $\mathbf{Z}$ para los que existe algún λ de $\mathbf{Z}$ tal que $x - 3 = \lambda 41$, es decir, $x = 3 + 41\lambda$. Así pues los x de $\mathbf{Z}$ tales que x es congruente con 3 módulo 41 son el conjunto $\{3 + 41\lambda \mid \lambda \in \mathbf{Z}\}$.

Ejemplo 3.5.4. Vamos ahora a hallar la solución del sistema de congruencias

$$\begin{array}{c} x \equiv 2 \text{ mód } 7 \\ x \equiv 5 \text{ mód } 9 \end{array} \tag{3.5.4.1}$$

es decir, vamos a encontrar todos los números enteros que son a la vez congruentes con 2 módulo 7 y con 5 módulo 9. Razonando como en el ejemplo 3.5.3, vemos que la solución de la primera congruencia de (3.5.4.1) es

$$x = 2 + 7\lambda. \tag{3.5.4.2}$$

Así pues, los números enteros que satisfacen (3.5.4.1) son los de la forma $x = 2 + 7\lambda$ donde λ cumple

$$2 + 7\lambda \equiv 5 \text{ mód } 9. \tag{3.5.4.3}$$

La congruencia (3.5.4.3) equivale a

$$7\lambda \equiv 3 \text{ mód } 9. \tag{3.5.4.4}$$

Por la observación 3.5.2, la congruencia (3.5.4.4) es equivalente a la igualdad $\overline{7\lambda} = \overline{3}$ en $\mathbf{Z}/(9)$. Como 7 y 9 son primos entre sí, por el corolario 3.4.9, el elemento $\overline{7}$ de $\mathbf{Z}/(9)$ es una unidad. De hecho, su inverso es $\overline{4}$, por lo que en $\mathbf{Z}/(9)$ tenemos

$$\overline{\lambda} = (\overline{4} \cdot \overline{7})\overline{\lambda} = \overline{4}(\overline{7\lambda}) = \overline{4} \cdot \overline{3} = \overline{3}.$$

La igualdad $\overline{\lambda} = \overline{3}$ en $\mathbf{Z}/(9)$ equivale a la congruencia

$$\lambda \equiv 3 \text{ mód } 9,$$

cuya solución es $\lambda = 3 + 9\mu$. Sustituyendo esta expresión en (3.5.4.2), obtenemos que los enteros que satisfacen (3.5.4.1) son de la forma $x = 2 + 7\lambda = 23 + 63\mu$, es decir, las soluciones del sistema (3.5.4.1) son los elementos del conjunto $\{23 + 63\mu \mid \mu \in \mathbf{Z}\}$.

Ejemplo 3.5.5. Vamos ahora a hallar la solución del sistema de congruencias

$$\begin{array}{l} x \equiv 5 \text{ mód } 27 \\ x \equiv 8 \text{ mód } 35 \end{array} \tag{3.5.5.1}$$

usando este vez el teorema 3.4.10. Según la observación 3.5.2, queremos encontrar todos los enteros x tales que su clase $x + (27)$ en $\mathbf{Z}/(27)$ sea igual a la clase de $5 + (27)$ y tales que su clase $x + (35)$ en $\mathbf{Z}/(35)$ sea igual a la clase de $8 + (35)$. Estos enteros son los que pertenecen a la imagen inversa de $(5 + (27), +(35)$ por el homomofismo

$$\begin{array}{rccc} \varphi: & \mathbf{Z} & \longrightarrow & \mathbf{Z}/(27) \times \mathbf{Z}/(35) \\ & x & \mapsto & (x + (27), y + (35)). \end{array}$$

De los teoremas 2.4.1 y 2.6.1 se sigue que $\varphi = \overline{\varphi} \circ \pi$, donde π es la proyección canónica de $\mathbf{Z}$ al anillo cociente $\mathbf{Z}/(945)$ y $\overline{\varphi}$ es el isomorfismo de (3.4.17.1). Por el cálculo realizado en el ejemplo 3.4.17 tenemos

$$\varphi^{-1}((5 + (27), 8 + (35))) = \pi^{-1}(\overline{\varphi}^{-1}((x + (27), y + (35)))) = \pi^{-1}(105 + (945)).$$

Así pues, los enteros x que satisfacen el sistema de congruencias (3.5.5.1) son aquellos cuya clase $x + (945)$ en $\mathbf{Z}/(945)$ es $105 + (945)$. Estos son los enteros x de la forma $x = 105 + 945\alpha$, para algún $\alpha \in \mathbf{Z}$.

Según lo visto en el ejemplo 3.5.4, el sistema (3.5.4.1) es equivalente a

$$x \equiv 23 \text{ mód } 63,$$

en el sentido de que ambos sistemas de congruencias tienen el mismo conjunto de soluciones enteras. De igual manera, según lo visto en el ejemplo 3.5.5, el sistema 3.5.5.1 es equivalente a

$$x \equiv 105 \text{ mód } 945.$$

Observamos que $63 = 7 \cdot 9$ y que $945 = 27 \cdot 35$. Todo esto lo podemos generalizar de la siguiente manera:

Teorema 3.5.6. *Sean $a_1, \ldots, a_n, m_1, \ldots, m_n \in \mathbf{Z}$ tales que m_i y m_j son primos entre sí para todo $i \neq j$. Sea $m = m_1 \cdots m_n$. El sistema de congruencias*

$$\begin{array}{rcl} x & \equiv & a_1 \text{ mód } m_1 \\ x & \equiv & a_2 \text{ mód } m_2 \\ \vdots & & \vdots \\ x & \equiv & a_n \text{ mód } m_n \end{array} \tag{3.5.6.1}$$

tiene una única solución módulo m. Esto quiere decir que existe un único número entero no negativo $0 < a \leq m$ *tal que el sistema* (3.5.6.1) *es equivalente a*

$$x \equiv a \text{ mód } m.$$

Demostración. Damos dos demostraciones del teorema 3.5.6. La primera, más elemental, usa los argumentos del ejemplo 3.5.4. Para ello observamos primero que como los $m_1, \ldots, m_n$ son primos dos a dos, para todo $1 \leq i \leq n-1$, se tiene que $m_1 \cdots m_i$ y m_{i+1} (esto es porque m_{i+1} no comparte factores primos con ninguno de los números $m_1, \ldots, m_i$, así que, por la unicidad de la decomposición en producto de factores primos, tanpoco comparte factores primos con $m_1 \cdots m_i$). Entonces, usando inducción en i, podemos reducir la demostración del teorema al caso $n = 2$. Argumentando como en el ejemplo 3.5.4, x satisface

$$\begin{array}{rcl} x & \equiv & a_1 \text{ mód } m_1 \\ x & \equiv & a_2 \text{ mód } m_2 \end{array} \tag{3.5.6.2}$$

si y solo si x es de la forma

$$x = a_1 + \alpha_1 m_1, \tag{3.5.6.3}$$

para algún entero α_1 tal que

$$\alpha_1 m_1 \equiv a_2 - a_1 \text{mód } m_2. \tag{3.5.6.4}$$

Por la observación 3.5.2, la congruencia (3.5.6.4) es equivalente a

$$\overline{\alpha}_1 \overline{m}_1 = \overline{a}_2 - \overline{a}_1 \text{ en } \mathbf{Z}/(m_2). \tag{3.5.6.5}$$

Como m_1 y m_2 son primos entre sí, por el corolario 3.4.9 la clase $\overline{m}_1$ es una unidad en $\mathbf{Z}/(m_2)$. Sea $\beta_1 \in \mathbf{Z}$ tal que $\overline{\beta}_1$ es el inverso de $\overline{m}_1$ en $\mathbf{Z}/(m_2)$. Entonces (3.5.6.5) equivale a

$$\overline{\alpha}_1 = \overline{\beta}_1(\overline{a}_2 - \overline{a}_1) \text{ en } \mathbf{Z}/(m_2)$$

y esto último a

$$\alpha_1 \equiv \beta_1(a_2 - a_1) \text{mód } m_2,$$

por lo que α_1 es de la forma

$$\alpha_1 = \beta_1(a_2 - a_1) + \alpha_2 m_2, \tag{3.5.6.6}$$

para algún entero α_2. Sustituyendo (3.5.6.6) en (3.5.6.7) concluimos que x es de la forma

$$x = a_1 + \beta_1(a_2 - a_1)m_1 + \alpha_2 m_1 m_2. \tag{3.5.6.7}$$

Si a es el resto entre 0 y $m_1 m_2 - 1$ de dividir $a_1 + \beta_1(a_2 - a_1)m_1$ entre $m_1 m_2$, vemos que las soluciones del sistema (3.5.6.2) son los x de la forma $x = a + \lambda m_1 m_2$, para algún entero λ, es decir, las soluciones de la congruencia

$$x \equiv a \text{ mód } m_1 m_2.$$

La segunda demostración se sigue de la versión para $\mathbf{Z}$ (corolario 3.4.11) del teorema chino del resto y de la observación 3.5.2. □

Tema 4

Factorialidad en anillos de polinomios

En este tema estudiaremos los anillos de polinomios y, concretamente, cuestiones sobre irreducibilidad y factorialidad en estos anillos. Entre otras cosas veremos criterios que nos darán condiciones suficientes y, a veces, también necesarias, para que un polinomio sea irreducible. También veremos que si R es un dominio de factorización única y K es su cuerpo de fracciones y $f(X)$ es un polinomio irreducible de $R[X]$, entonces $f(X)$ también es irreducible en $K[X]$. Este resultado, debido a Gauss, nos servirá para demostrar que si R es un dominio de factorización única, entonces $R[X]$ también es un dominio de factorización única (como consecuencia de esto, si $\mathbf{k}$ es un cuerpo, entonces $\mathbf{k}[X_1, \ldots, X_n]$ es un dominio de factorización única para todo $n \in \mathbf{N}$).

4.1 Raíces de un polinomio

Definición 4.1.1. Sean R y S anillos tales que R es un subanillo de S y sea $f(X) \in R[X]$. Decimos que $\alpha \in S$ es una *raíz* de f si $f(\alpha) = 0$.

Ejemplos 4.1.2. (1) Sea $f(X) = X^2 - 1 \in \mathbf{Z}[X]$. Entonces 1 y -1 son raíces de $f(X)$.

(2) Sea $f(X) = X^3 - 5 \in \mathbf{Z}[X]$. Entonces $\sqrt[3]{5}$ (que pertenece a $\mathbf{R}$) es una raíz de $f(X)$. Es fácil ver (por ejemplo con argumentos de análisis básico) que $f(X)$ no tiene otras raíces reales. El polinomio $f(X)$ no tiene ninguna raíz entera.

(3) Sea $f(X) = X^2 + 1 \in \mathbf{Z}[X]$. Entonces i y $-i$ (que pertenecen a $\mathbf{C}$) son raíces de $f(X)$. Es claro que $f(X)$ no tiene raíces reales y, por tanto, no tiene raíces enteras.

Proposición 4.1.3. *Sea R anillo y sea $f(X) \in R[X]$, $f \neq 0$. Entonces $\alpha \in R$ es una raíz de $f(X)$ si y solo si $(X - \alpha)$ divide $f(X)$ en $R[X]$.*

Demostración. Si $(X - \alpha)$ divide $f(X)$ en $R[X]$, entonces existe $g(X) \in R[X]$ tal que $f(X) = g(X)(X - \alpha)$, así que, al evaluar esa igualdad en α tenemos $f(\alpha) = g(\alpha) \cdot 0 = 0$. Sea ahora $\alpha \in R$ raíz de $f(X)$. Como R es un anillo arbitrario, R no tiene por qué ser un cuerpo, por lo que $R[X]$ no tiene por qué ser un dominio euclídeo. A pesar de ello,

como $X - \alpha$ es un polinomio *mónico*[1] de $R[X]$, podemos dividir $f(X)$ entre $X - \alpha$ usando el algoritmo de división de polinomios y obtenemos $f(X) = g(X)(X - \alpha) + r(X)$, donde $g(X), r(X) \in R[X]$ y $r(X)$ tiene grado menor que 1 en X, es decir, $r(X)$ es una constante r de R. Como $f(\alpha) = 0$, se sigue que $r = 0$ y $f(X) = g(X)(X - \alpha)$. □

Corolario 4.1.4. *Sea R un dominio de integridad y sea $f(X) \in R[X]$ de grado mayor que 1. Si $f(X)$ tiene alguna raíz en R, entonces $f(X)$ es un elemento reducible de $R[X]$.*

Demostración. Sea $n \geq 2$ el grado de $f(X)$. Si $\alpha \in R$ es una raíz de $f(X)$, entonces por la proposición 4.1.3, existe $g(X) \in R[X]$ tal que $f(X) = g(X)(X - \alpha)$. Como $X - \alpha$ tiene grado 1, tenemos que $g(X)$ tiene grado $n - 1 > 0$. Como $U(R[X]) = U(R)$, las unidades de $R[X]$ tienen grado 0, así que ni $X - \alpha$ ni $g(X)$ son unidades. □

Corolario 4.1.5. *Sea $\mathbf{k}$ cuerpo y sea $f(X) \in \mathbf{k}[X]$, $f \neq 0$. Entonces $f(X)$ tiene alguna raíz en $\mathbf{k}$ si y solo si $f(X)$ tiene algún factor lineal (es decir, de grado 1) en $\mathbf{k}[X]$.*

Demostración. Si f tiene una raíz $\alpha \in \mathbf{k}$, entonces $X - \alpha$ es un factor de f en $\mathbf{k}[X]$ por la proposición 4.1.3. Sea ahora $aX - b \in \mathbf{k}[X]$ un factor de grado 1 de f en $\mathbf{k}[X]$. Entonces $a \neq 0$, por lo que $a^{-1} \in \mathbf{k}$ y $\alpha = a^{-1}b \in \mathbf{k}$ es un raíz de f. □

Resumimos en la proposición siguiente lo que nos dice la existencia de raíces de un polinomio $f(X)$ de $\mathbf{k}[X]$ sobre la irreducibilidad de $f(X)$:

Proposición 4.1.6. *Sea $\mathbf{k}$ cuerpo y sea $f(X) \in \mathbf{k}[X]$, $f \neq 0$.*

(1) El polinomio f es una unidad de $\mathbf{k}[X]$ si y solo si el grado de f es 0.

(2) Si el grado de f es 1, entonces f es un elemento irreducible de $\mathbf{k}[X]$.

(3) Si el grado de f es 2 o 3, entonces f es un elemento irreducible de $\mathbf{k}[X]$ si y solo si f no tiene raíces en $\mathbf{k}$.

(4) Si el grado de f es mayor que 3 y f tiene alguna raíz en R, entonces f es un elemento reducible de $\mathbf{k}[X]$.

Demostración. El apartado (1) ya es conocido, ya que $U(\mathbf{k}[X]) = U(\mathbf{k}) = \mathbf{k} \setminus \{0\}$.

Si f tiene grado 1 y $f = g \cdot h, g, h \in \mathbf{k}[X]$, entonces el grado de g es 1 y el de h es 0 o viceversa, porque $\mathbf{k}$ es un cuerpo; por ello, g o h son unidades por el apartado (1). Esto prueba (2).

Sea f de grado 2 o 3. Si f tiene una raíz ya vimos en el corolario 4.1.4 que f es reducible. Supongamos ahora que f es reducible. Entonces existen $g, h \in \mathbf{k}[X]$ tales que $f = gh$ y ni g ni h son unidades, por lo que, por (1), los grados de f y g son positivos. Como $\mathbf{k}$ es un cuerpo, los grados de g y h suman 2 si el grado de f es 2 y 3 si el grado de f es 3, por lo que g o h es un polinomio de grado 1. En ese caso concluimos el argumento usando el corolario 4.1.5.

El apartado (4) es consecuencia directa del corolario 4.1.4. □

[1] es decir, con coeficiente 1 en su término de mayor grado

Ejemplos 4.1.7. (1) El polinomio $f(X) = X^2 + X + 1$ de $\mathbf{Z}_5[X]$ no tiene raíces en $\mathbf{Z}_5$ (la evalución de $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$ en $f(X)$ es respectivamente $\overline{1}, \overline{3}, \overline{2}, \overline{3}, \overline{1}$), por lo que $f(X)$ es un polinomio irreducible de $\mathbf{Z}_5[X]$ por la proposición 4.1.6 (3).

(2) El polinomio $f(X) = X^3 + 2X^2 - X + 3$ de $\mathbf{Z}[X]$ no tiene raíces en $\mathbf{Q}$. En efecto, según el ejercicio 1 de la hoja 4, las posibles raíces racionales de $f(X)$ son $1, -1, 3$ y -3, y al evaluar $f(X)$ en ellas obtenemos $5, 5, 45$ y -3 respectivamente. En ese caso, la proposición 4.1.6 (3) nos dice que $f(X)$ es irreducible en $\mathbf{Q}[X]$.

(3) El polinomio $f(X) = X^4 + 3X^2 + 2 = (X^2 + 1)(X^2 + 2) \in \mathbf{R}[X]$ no tiene raíces en $\mathbf{R}$ pero es reducible el $\mathbf{R}[X]$. Este ejemplo muestra que el recíproco del apartado (4) de la proposición 4.1.6 es falso.

4.2 El criterio modular

Observación 4.2.1. Sea $\sigma : R \longrightarrow S$ un homomorfismo de anillos.

(1) La aplicación σ^*

$$\begin{array}{ccc} R[X] & \xrightarrow{\sigma^*} & S[X] \\ f & \mapsto & \sigma^*(f), \end{array}$$

donde $f = a_0 + a_1X \cdots + a_nX^n$ y $\sigma^*(f) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n$, es un homomorfismo de anillos.

(2) El grado de $\sigma^*(f)$ es menor o igual que el grado de f.

Proposición 4.2.2. *Sea R un anillo, sea S un dominio de integridad y sea $\sigma : R \longrightarrow S$ un homomorfosmo de anillos. Sea $f(X) \in R[X]$, $f \neq 0$. Si*

(i) el grado de f es igual al grado de $\sigma^*(f)$; y

(ii) $\sigma^*(f)$ es irreducible en $S[X]$,

entonces $f(X)$ no se puede escribir como producto de dos polinomios de $R[X]$ ambos de grado menor que el grado de f.

Demostración. Hacemos la demostración por reducción al absurdo. Así, supongamos que existen $g, h \in R[X]$ tales que $f = gh$ y tales que los grados de g y h son menores que el grado de f y lleguemos a una contradicción. En $S[X]$ tenemos $\sigma^*(f) = \sigma^*(g)\sigma^*(h)$, ya que σ^* es un homomorfismo de anillos. Como por (ii) $\sigma^*(f)$ es irreducible en $S[X]$, $\sigma^*(g)$ o $\sigma^*(h)$ es una unidad en $S[X]$. Supongamos por ejemplo que la unidad es $\sigma^*(g)$. Como $U(S[X]) = U(S)$, el grado de $\sigma^*(g)$ es 0. Entonces el grado de $\sigma^*(f)$ es la suma de los grados de $\sigma^*(g)$ y $\sigma^*(h)$, ya que S es un dominio de integridad y, como el grado de $\sigma^*(g)$ es 0, el grado de $\sigma^*(f)$ es igual al grado de $\sigma^*(h)$, que es menor o igual que el grado de h, que a su vez, por nuestra suposición inicial, es menor que el grado de f. Obtenemos por

tanto que el grado de $\sigma^*(f)$ es menor que el grado de f y esto contradice (i). Por tanto no pueden existir $g, h \in R[X]$ tales que $f = gh$ y tales que los grados de g y h sean menores que el grado de f. □

Corolario 4.2.3. *(Criterio modular). Sea R un anillo y sea $\mathfrak{p}$ un ideal primo de R. Sea $f(X) = a_0 + a_1X + \cdots a_nX^n \in R[X]$, con $a_n \neq 0$. Sea $\overline{a_i}$ la clase de a_i en $R/\mathfrak{p}$. Si*

(i) $a_n \notin \mathfrak{p}$; y

(ii) $\overline{a_0} + \overline{a_1}X + \cdots \overline{a_n}X^n$ es irreducible en $(R/\mathfrak{p})[X]$,

entonces $f(X)$ no se puede escribir como producto de dos polinomios de $R[X]$ ambos de grado menor que n.

Demostración. Sea

$$\sigma = \pi : R \longrightarrow R/\mathfrak{p}$$

la proyección canónica desde R al cociente $R/\mathfrak{p}$. Entonces $\sigma^*(f) = \overline{a_0} + \overline{a_1}X + \cdots \overline{a_n}X^n$. Que $a_n \notin \mathfrak{p}$ es equivalente a que $\overline{a_n} \neq \overline{0}$ en $R/\mathfrak{p}$ y esto equivale a que $\sigma^*(f)$ tenga el mismo grado que f, esto es, a la condición (i) de la proposición 4.2.2. Por otra parte, la condición (ii) del corolario 4.2.3 es exactamente lo mismo que la condición (ii) de la proposición 4.2.2. □

Observación 4.2.4. Sea R un dominio de integridad y sea $f(X)$ un polinomio de $R[X]$ de grado n, $n \in \mathbf{N}$. La condición de que $f(X)$ no pueda escribrise como producto de dos polinomios de $R[X]$ ambos de grado menor que n es equivalente a la condición de que $f(X)$ no pueda escribrise como producto de dos polinomios de $R[X]$ ambos de grado positivo.

Ejemplo 4.2.5. Un caso típico en el que se usa el corolario 4.2.3 es cuando $R = \mathbf{Z}$ y $\mathfrak{p} = (p)$, donde p es un número primo. Usamos dicho corolario para ver que el polinomio $f(X) = 8X^3 - 6X - 1$ de $\mathbf{Z}[X]$ no se puede escribir como producto de dos polinomios de $\mathbf{Z}[X]$ ambos de grado menor que 3.

No podemos aplicar el criterio modular para $p = 2$ porque 2 divide a 8, por lo que no se cumple la condición (i).

Intentamos aplicar el criterio modular para $p = 3$. En este caso $\sigma^*(f) = \overline{2}X^3 - \overline{1} \in (\mathbf{Z}/(3))[X]$ es reducible, ya que tiene a $\overline{2} \in \mathbf{Z}/(3)$ como raíz. Por tanto no se cumple la condición (ii) por lo que tampoco podemos aplicar el criterio.

Intentamos aplicar el criterio modular para $p = 5$. En este caso $\sigma^*(f) = \overline{3}X^3 - X - \overline{1} \in (\mathbf{Z}/(5))[X]$ tiene grado 3, por lo que se cumple la condición (i), y es irreducible en $(\mathbf{Z}/(5))[X]$, ya que tiene grado 3 y no tiene raíces en $\mathbf{Z}/(5)$ (esto último se puede comprobar evaluando $\sigma^*(f)$ en los cinco elementos de $\mathbf{Z}/(5)$), por lo que se cumple la condición (ii). Por tanto $f(X)$ no se puede escribir como producto de dos polinomios de $\mathbf{Z}[X]$ ambos

de grado menor que 3 o, lo que es lo mismo, no se puede escribir como producto de dos polinomios de $\mathbf{Z}[X]$ ambos de grado positivo.

Como el máximo común divisor de los coeficientes de $f(X)$ es 1, $f(X)$ es un polinomio *primitivo* de $\mathbf{Z}[X]$ (véase la definición 4.3.2). Entonces, por la proposición 4.3.4, $f(X)$ es un polinomio irreducible de $\mathbf{Z}[X]$.

4.3 Irreducibilidad en $R[X]$ frente a irreducibilidad en $K[X]$

Convenio 4.3.1. En lo que resta de tema R denotará un dominio de factorización única y K denotará el cuerpo de fracciones de R.

Queremos responder a la siguiente pregunta: si $f(X) \in R[X]$ es irreducible en $R[X]$, ¿será $f(X)$ irreducible en $K[X]$? No sabemos la respuesta a priori, ya que al pasar de R a K estamos ampliando el anillo de coficientes de nuestros polinomios. Eso hace que existan más polinomios en $K[X]$ que en $R[X]$ por lo que, aunque $f(X)$ no se pueda factorizar en $R[X]$ quizá sí se pueda factorizar en $K[X]$. Aunque el caso es distinto al que tratamos ahora, ya que $\mathbf{C}$ no es el cuerpo de fracciones de $\mathbf{R}$ ($\mathbf{R}$ ya es un cuerpo por lo que su cuerpo de fracciones es él mismo), el siguiente ejemplo ilustra por qué el ampliar el anillo de coeficientes podría cambiar el carácter irreducible de un polinomio: el polinomio X^2+1 es irreducible en $\mathbf{R}[X]$ pero es reducible en $\mathbf{C}[X]$, ya que en $\mathbf{C}[X]$ admite la factorización $X^2+1 = (X+i)(X-i)$, factorización que no es válida en $\mathbf{R}[X]$ ya que $i \notin \mathbf{R}$. En esta sección veremos en cambio que si $f(X) \in R[X]$ es irreducible, entonces $f(X)$ también es irreducible en $K[X]$ [2]. Como consecuencia de este hecho, veremos que si R es un dominio de factorización única, entonces $R[X]$ también es dominio de factorización única.

Definición 4.3.2. Sea $f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ (es decir, $a_0, a_1, \ldots, a_n \in R$), polinomio no nulo. Decimos que f es *primitivo* si 1 es máximo común divisor de los elementos no nulos de $\{a_0, a_1, \ldots, a_n\}$.

Observación 4.3.3. Si d es máximo común divisor de los coeficientes no nulos de un polinomio $f(X) \in R[X]$, entonces el polinomio $\frac{1}{d}f(X)$ (que, en principio, es un polinomio de $K[X]$) es un polinomio primitivo de $R[X]$.

Proposición 4.3.4. *Sea $f(X) \in R[X], f \neq 0, f \notin U(R[X])$. Entonces f es un elemento irreducible de $R[X]$ si y solo si f es primitivo y no se puede escribir como producto de dos polinomios de $R[X]$ ambos de grado positivo.*

[2] La razón heurística de esto es que, en realidad, la ampliación de R a K consiste esencialmente en convertir todos los elementos no nulos de R en unidades de K. Al haber en K más unidades, es más "fácil" ser irreducible en $K[X]$ que en $R[X]$. De hecho, existirán factorizaciones $g \cdot h$ que en $R[X]$ violan la irreducibilidad pero no lo hacen en $K[X]$, por ser g o h unidades en $K[X]$. Esto nos daría ejemplos de elementos de $R[X]$, irreducibles en $K[X]$ pero no en $R[X]$ (véase la proposición 4.3.4 y el ejemplo 4.3.5). Así pues, el recíproco de la afirmación que motiva esta nota a pie de página es falso.

Demostración. Demostraremos que f es reducible en $R[X]$ si y solo si f no es primitivo o f se puede escribir como producto de dos polinomios de $R[X]$ ambos de grado positivo. Supongamos primero que f es reducible. Entonces existen $g, h \in R[X], f, g \notin U(R[X])$ tales que $f(X) = g(X)h(X)$. Si tanto el grado de g como el grado de h son positivos, no hay nada que demostrar. Supongamos entonces que, por ejemplo, g tiene grado 0. Como $U(R[X]) = U(R)$, entonces $g = a \in R$ y $a \notin U(R)$. Entonces $f = ah$, por lo que a divide a todos los coeficientes de f y, por tanto, al máximo común divisor de los coeficientes no nulos de f. Entonces ese máximo común divisor no puede ser 1, pues si lo fuera a sería unidad. Así pues, f no es primitivo.

Supongamos ahora que f se escribe como producto de dos polinomios g y f de $R[X]$ de grado positivo. En ese caso $g, h \notin U(R[X])$, por lo que f es reducible. Finalmente supongamos que f no es primitivo. Entonces el máximo común divisor d de los coeficientes no nulos de f no es una unidad. Como

$$f = d \cdot (\frac{1}{d} f(X)) \tag{4.3.4.1}$$

y $\frac{1}{d} f(X) \in R[X]$ por la observación 4.3.3 y no es unidad, pues f no lo es, (4.3.4.1) nos dice que f es reducible. □

Ejemplo 4.3.5. Aunque el polinomio $2X$ de $\mathbf{Z}[X]$ no se puede escribir como producto de dos polinomios de $\mathbf{Z}[X]$ ambos de grado positivo, no es irreducible en $\mathbf{Z}[X]$ ya que no es primitivo.

Proposición 4.3.6. *(Lema de Gauss). Si $f(X), g(X)$ son dos polinomios primitivos de $R[X]$, entonces $f \cdot g$ es también primitivo.*

Demostración. Supongamos que $f \cdot g$ no fuera primitivo. Entonces un máximo común divisor de los coeficientes no nulos de $f \cdot g$ (ese máximo común divisor existe ya que $R[X]$ es un dominio de integridad, por lo que $f \cdot g \neq 0$ así que $f \cdot g$ posee algún coeficiente no nulo) sería un elemento $a \in R$, distinto de 0 y no unidad. Como R es un dominio de factorización única, a tiene una descomposición finita como producto de irreducibles, y en particular existe $p \in R$ irreducible tal que p divide a a. Como R es un dominio de factorización única, el ideal (p) de R es primo (véase la proposición 3.3.8 y la observación 3.3.9), por lo que $S = R/(p)$ es un dominio de integridad. Sea σ la proyección canónica

$$\begin{array}{rccc} \sigma: & R & \longrightarrow & S \\ & b & \mapsto & \overline{b} \end{array}$$

y sea σ^* el homomorfismo de anillos definido en la observación 4.2.1. Tenemos entonces que, como todos los coeficientes de $f \cdot g$ son múltiplos de p, $\sigma^* f \cdot \sigma^* g = \sigma^*(f \cdot g) = 0$ en $S[X]$. Por otra parte, como f es primitivo (es decir, un máximo común divisor de sus coeficientes es 1), p no puede dividir a todos sus coeficientes (pues si lo hiciera, dividiría también a 1, pero entonces p sería unidad). Pero si p no divide a algún coeficiente a_i de f, entonces $\sigma(a_i)$ es un elemento no nulo de $S = R/(p)$, por tanto $\sigma^* f \neq 0 \in S[X]$. Igual

ocurre con g: $\sigma^* g \neq 0 \in S[X]$. Pero S es un dominio de integridad y por tanto $S[X]$ también lo es, por lo que tenemos una contradicción. □

Proposición 4.3.7. *Sea $f(X) \in K[X]$, $f \neq 0$.*

(1) Existen $c \in K \setminus \{0\}$ y $f^* \in R[X]$ tales que f^* es primitivo y $f = cf^*$.

(2) Si $c, c' \in K \setminus \{0\}$ y $f^*, h \in R[X]$ son tales que f^* y h son primitivos y $f = cf^* = c'h$, entonces existe $u \in U(R)$ tal que $c' = u \cdot c$ y $h = u^{-1} f^*$, es decir, la descomposición del apartado (1) es única salvo producto por unidad.

Demostración. Para ver (1), si $b \in R$ es el producto de los denominadores de los coeficientes (no nulos) de $f(X)$, claramente $bf \in R[X]$. Sea ahora $d \in A$ un máximo común divisor de los coeficientes de bf. Entonces definimos f^* como $\frac{b}{d} f$ que, según la observación 4.3.3 es un polinomio primitivo de $R[X]$. Entonces $c = \frac{d}{b} \in K \setminus \{0\}$, y $f = cf^*$ cumple (1).

Para ver (2), si $cf^* = c'h$, consideramos $c/c' = r/s$, con $r, s \in R$ tales que el máximo común divisor de r y s sea una unidad. Entonces $rf^* = sh$. Sean b_i los coeficientes de h. Entonces r divide a cada uno de los coeficientes $s \cdot b_i$ de sh. Si r no es una unidad, comparando una descomposición como producto de irreducibles de r con una descomposición en producto de irreducibles de $s \cdot b_i$, se deduce que r divide a b_i para todo b_i. Como h es primitivo, r ha de ser unidad, pero habíamos supuesto que no lo era, con lo que llegamos a una contradicción por esta suposición, por lo que r es unidad. Como f^* es también primitivo podemos hacer el mismo argumento para deducir que $s \in U(R)$. Entonces, en K, $s/r = s \cdot r^{-1}$, por lo que $s/r \in R$ y, de hecho, es una unidad de A. Como $c'/c = s/r$, si denotamos $u = c'/c$, entonces $u \in U(R)$, $c' = uc$ y $h = u^{-1} f^*$. □

Definición 4.3.8. A cualquier constante $c \in K \setminus \{0\}$ que cumpla la condición (1) de la proposición 4.3.7 la llamaremos *contenido* de f (según hemos visto en la proposición 4.3.7 (2), el contenido de f es único salvo producto por una unidad).

Proposición 4.3.9. *Si $f(X) \in R[X]$, entonces el contenido de f pertenece a R.*

Demostración. Sea $d \in R$ máximo común divisor de los coeficientes de $f(X)$. En ese caso el polinomio $g = \frac{1}{d} f$ está en $R[X]$ y es primitivo por la observación 4.3.3. En ese caso $f = dg$ es una descomposición de f como la que aparece en el apartado (1) de la proposición 4.3.7 por lo que podemos tomar d como el contenido de f y $d \in R$. Cualquier otra constante $c \in K$ que cumpla (1) de la proposición 4.3.7 es de la forma $d = uc$, donde $u \in U(R)$, por lo que, en particular, $c \in R$. □

Proposición 4.3.10. *Sean $f(X), g(X), h(X) \in K[X]$ tales que $f = g \cdot h$. Sean $d, e \in K$ y $g^*(x), h^*(x) \in R[X]$ tales que d, e, g^*, h^* cumplen (1) de la proposición 4.3.7 (en particular, d se puede tomar como el contenido de g y e como el contenido de h). Entonces $c = d \cdot e$ y $f^* = g^* \cdot h^*$ cumplen (1) de la proposición 4.3.7; en particular, $d \cdot e$ se puede tomar como el contenido de f.*

Demostración. Tenemos que $f = g \cdot h = (dg^*) \cdot (eh^*) = (d \cdot e)(g^* \cdot h^*)$. Por la proposición 4.3.6, $g^* \cdot h^*$ es un polinomio primitivo de $R[X]$. Por tanto $c = d \cdot e$ y $f^* = g^* \cdot h^*$ cumplen (1) de la proposición 4.3.7. □

Teorema 4.3.11. *(Gauss). Sea $f(X) \in R[X]$, $f \neq 0$. Si $f(X)$ no se puede escribir como producto de dos polinomios de $R[X]$ ambos de grado positivo, entonces $f(X)$ es un elemento irreducible de $K[X]$.*

Demostración. Demostraremos que si $f(X)$ es reducible en $K[X]$, entonces se puede obtener una descomposición de $f(X)$ como producto de dos polinomios de $R[X]$ ambos de grado positivo. Recordemos que $U(K[X]) = U(K)$. Como K es un cuerpo, $U(K) = K \setminus \{0\}$, es decir, las unidades de $K[X]$ son los polinomios constantes distintos de 0. Si $f(X)$ es reducible en $K[X]$, existen $g(X), h(X) \in K[X]$, no unidades, tales que $f = gh$. Como $g(X)$ y $h(X)$ no son unidades, su grado es positivo. Veamos ahora que a partir de la descomposición $f = gh$ en $K[X]$ podemos obtener una descomposición de f en $R[X]$. Existen $d, e \in K$ y $g^*, h^* \in R[X]$ primitivos que cumplen (1) de la proposición 4.3.7. Por la proposición 4.3.10, podemos tomar de como el contenido de f. Por la proposición 4.3.9, $de \in R$, pues $f \in R[X]$ por hipótesis. Tenemos pues la descomposición

$$f(X) = ((de) \cdot g^*(X)) \cdot h^*(X) \tag{4.3.11.1}$$

de f en $R[X]$, ya que $g' := ((de) \cdot g^*(X))$ y $h^*(X)$ pertenecen a $R[X]$. Por otra parte, en $K[X]$ tenemos las igualdades $g' = eg$ y $h^* = e^{-1}h$, por lo que g' tiene el mismo grado que g y h^* tiene el mismo grado que h. Por tanto g' y h^* son polinomios de $R[X]$ de grado positivo. Entonces (4.3.11.1) demuestra que f se puede escribir como producto de dos polinomios de $R[X]$ ambos de grado positivo. □

Corolario 4.3.12. *Si $f(X)$ es un polinomio irreducible en $R[X]$, entonces $f(X)$ es un polinomio irreducible en $K[X]$.*

Demostración. Si $f(X)$ es un polinomio irreducible en $R[X]$, $f(X)$ no se puede escribir como producto de polinomios de $R[X]$ de grado positivo, por la proposición 4.3.4. Entonces, por el teorema 4.3.11, $f(X)$ es un polinomio irreducible en $K[X]$. □

Corolario 4.3.13. *Sea $f(X)$ un polinomio de $R[X]$. Entonces $f(X)$ es irreducible en $K[X]$ si y solo si no se puede escribir como producto de polinomios de $R[X]$ de grado positivo.*

Demostración. Una de las dos implicaciones es el teorema 4.3.11. Para la otra implicación, supongamos que $f(X)$ es irreducible en $K[X]$. Si $g(X)$ y $h(X)$ son polinomios de $R[X]$ de grado positivo tales que $f(X) = g(X)h(X)$, entonces $g(X) \notin U(K[X])$ y $h(X) \notin U(K[X])$, por lo que $f(X)$ sería un polinomio reducible de $K[X]$. □

4.4 Si R es un dominio de factorización única, entonces $R[X]$ es un dominio de factorización única

Vemos en esta sección la consecuencia más importante del lema y del teorema de Gauss: que si R es un dominio de factorización única, entonces $R[X]$ es un dominio de factorización única. Antes de demostrar esto necesitamos el siguiente lema:

Lema 4.4.1. *Sea $f(X) \in K[X]$ y sea $f^*(X) \in R[X]$ polinomio primitivo que cumple (1) de la proposición 4.3.7. Si $f(X)$ es un elemento irreducible de $K[X]$, entonces $f^*(X)$ es un elemento irreducible de $R[X]$.*

Demostración. Vemos que si f^* es reducible en $R[X]$, entonces f es reducible en $K[X]$. Como f^* es primitivo, la proposición 4.3.4 implica que $f^* = g \cdot h$, donde g, h son polinomios de $R[X]$ de grado positivo. Sea $c \in K$ tal que $f = cf^*$. Por el corolario 4.3.13, f^* es reducible en $K[X]$ y $f = cf^*$ también. □

Teorema 4.4.2. *Si R es un dominio de factorización única entonces $R[X]$ también es un dominio de factorización única.*

Demostración. Usamos el corolario 3.3.11. Demostramos primero que $R[X]$ cumple la propiedad (i') del corolario 3.3.11. Sea $f(X) \in R[X]$ no nulo y no unidad. Si $f(X)$ tiene grado 0, entonces es un polinomio constante $f(X) = a$, con $a \in R$, $a \neq 0$. Como $U(R[X]) = U(R)$, $a \notin U(R)$. Como R es un dominio de factorización única, a posee una descomposición en producto finito de elementos irreducibles en R. Esta descomposición nos proporciona una descomposición de $f(X)$ como producto de polinomios (constantes) irreducibles de $R[X]$. Esto es así porque si $p \in R$ es un elemento irreducible de R, el polinomio constante p es un elemento irreducible de $R[X]$ ya que dicho polinomio solo se puede poner como producto de dos polinomios si estos son constantes y, como p es un elemento irreducible de R, uno de esos dos polinomios es una unidad en $R[X]$.

Razonamos ahora para el caso en que el grado de $f(X)$ sea mayor que 0. Recordemos que K es el cuerpo de fracciones de R. Como K es un cuerpo, $K[X]$ es un dominio euclídeo y por tanto un dominio de factorización única. Entonces, si consideramos $f(X)$ en $K[X]$, tenemos que $f(X) = g_1(X) \cdots g_n(X)$, donde $g_1, \ldots, g_n$ son polinomios de $K[X]$ irreducibles. A partir de esta factorización queremos producir una factorización en $R[X]$ ($g_1, \ldots, g_n$ no tienen por qué estar en $R[X]$). Por la proposición 4.3.7 (1) existen $c_1, \ldots, c_n \in K$ y $g_1^*(X), \ldots, g_n^*(X) \in R[X]$ primitivos tales que $g_i = c_i \cdot g_i^*$. Por el lema 4.4.1, $g_1^*(X), \ldots, g_n^*(X)$ son polinomios irreducibles de $R[X]$. Por la proposición 4.3.6 el producto $g_1^*(X) \cdots g_n^*(X)$ es un polinomio primitivo de $R[X]$. Por la proposición 4.3.10, podemos tomar $c = c_1 \cdots c_n$ como contenido de $f(X)$ y la descomposición $f(X) = c \cdot (g_1^*(X) \cdots g_n^*(X))$ cumple (1) de la proposición 4.3.7. Como $f(X) \in R[X]$, por la proposición 4.3.9, $c \in R$. Si $c \in U(R)$, entonces $f(X) = (cg_1^*(X)) \cdots g_n^*(X)$ es una factorización como producto de elementos irreducibles de $R[X]$. Como R es un dominio de factorización única, si $c \notin U(R)$, entonces existen $p_1, \ldots, p_k \in R$ irreducibles tales que $c = p_1 \cdots p_k$. Entonces $f(X) =$

$p_1 \cdots p_k \cdot g_1^*(X) \cdots g_n^*(X)$ es una factorización como producto de elementos irreducibles de $R[X]$.

Demostramos ahora que $R[X]$ cumple la propiedad (ii') del corolario 3.3.11. Sea $f(X)$ un elemento irreducible de $R[X]$. Si $f(X) = p$ es un polinomio constante, entonces p es un elemento irreducible de R. Sean $g(X)$ y $h(X)$ polinomios de $R[X]$ tales que $f(X)$ divide a $g(X)h(X)$ en $R[X]$. Eso quiere decir que p divide (en R) a todos los coeficientes de $g(X)h(X)$. Entonces, usando el mismo argumento y el mismo homomorfismo σ^* de la demostración de la proposición 4.3.6, se tiene que $\sigma^* g = 0$ o $\sigma^* h = 0$. Si, por ejemplo, $\sigma^* g = 0$, p divide a todos los coeficientes de $g(X)$ o, lo que es lo mismo, f divide a g (en $R[X]$). Por tanto f es un elemento primo de $R[X]$.

Sea ahora $f(X)$ un polinomio irreducible en $R[X]$ de grado mayor que 0. Sean $g(X)$ y $h(X)$ polinomios de $R[X]$ tales que $f(X)$ divide a $g(X)h(X)$ en $R[X]$. Entonces existe $\lambda(X) \in R[X]$ tal que $gh = \lambda f$, así que también tenemos que $f(X)$ divide a $g(X)h(X)$ en $K[X]$. Por otra parte, $f(X)$ es irreducible en $R[X]$ luego, por el corolario 4.3.12, $f(X)$ es irreducible en $K[X]$. Como $K[X]$ es un dominio de factorización única, $K[X]$ cumple la propiedad (ii') del corolario 3.3.11 y, en $K[X]$, o bien $f(X)$ divide a $g(X)$, o bien $f(X)$ divide a $h(X)$. Digamos, por ejemplo, que $f(X)$ divide a $g(X)$ en $K[X]$. Entonces existe $\mu(X) \in K[X]$ tal que $g(X) = \mu(X) \cdot f(X)$. Sea $m \in K$ contenido de $\mu(X)$ y sea $\mu^* \in R[X]$ polinomio primitivo que cumplen (1) de la proposición 4.3.7. Como $f(X)$ es irreducible en $R[X]$, $f(X)$ es primitivo por la proposición 4.3.4. Por la proposición 4.3.6, $\mu^* \cdot f$ es primitivo. Entonces, la descomposición $g = m \cdot (\mu^* f)$ cumple (1) de la proposición 4.3.7 y podemos tomar m como el contenido de g. Como $g(X) \in R[X]$, por la proposición 4.3.9, $m \in R$. Entonces, en realidad $\mu(X) = m \cdot \mu^*(X) \in R[X]$, por lo que $g(X)$ divide a $f(X)$ también en $R[X]$. □

Corolario 4.4.3. *Si R es un dominio de factorización única, entonces $R[X_1, \ldots, X_n]$ es un dominio de factorización única. En particular, $\mathbf{Z}[X_1, \ldots, X_n]$ es un dominio de factorización única y, si $\mathbf{k}$ es un cuerpo, $\mathbf{k}[X_1, \ldots, X_n]$ es un dominio de factorización única.*

Demostración. El corolario se demuestra usando inductivamente el teorema 4.4.2. Como $\mathbf{Z}$ y, trivialmente, un cuerpo $\mathbf{k}$ son dominios euclídeos, son dominios de factorización única, por lo que $\mathbf{Z}[X_1, \ldots, X_n]$ y $\mathbf{k}[X_1, \ldots, X_n]$ son dominios de factorización única. □

4.5 El criterio de Eisenstein

Lema 4.5.1. *Sea S un dominio de integridad, sea $a \in S$, $a \neq 0$ y sea $n \in \mathbf{N}$. Sean $g(X), h(X) \in S[X]$. Si $aX^n = g(X)h(X)$, entonces $g(X) = bX^m$ y $h(X) = cX^l$, donde $b, c \in S$ y $m, l \in \mathbf{N}$. En ese caso, $bc = a$ y $m + l = n$.*

Demostración. Demostramos el lema por contraposición. Supongamos que $g(X)$ o $h(X)$ tiene al menos dos monomios (de grados distintos). Como S es un dominio de integridad, el producto del monomio de menor grado de $g(X)$ por el monomio de menor grado de

$h(X)$ es un monomio no nulo y, de hecho, es el monomio de menor grado de $g(X)h(X)$. Como S es un dominio de integridad, el producto del monomio de mayor grado de $g(X)$ por el monomio de mayor grado de $h(X)$ es un monomio no nulo y, de hecho, es el monomio de mayor grado de $g(X)h(X)$. Como $g(X)$ o $h(X)$ tiene al menos dos monomios, el monomio de menor grado y el monomio de mayor grado de $g(X)h(X)$ tienen grados distintos, por lo que no puede ser $aX^n = g(X)h(X)$, pues en ese caso $g(X)h(X)$ tendría un solo monomio. □

Teorema 4.5.2. *Sea R un dominio de factorización única, sea K su cuerpo de fracciones y sea $f(X) = a_0 + a_1X + \cdots + a_nX^n$ un polinomio de grado n de $R[X]$. Sea p un elemento irreducible de R. Si*

(i) p divide a $a_0, a_1, \ldots, a_{n-1}$;

(ii) p no divide a a_n; y

(iii) p^2 no divide a a_0,

entonces $f(X)$ no puede escribirse como producto de dos polinomios de $R[X]$ de grado positivo y, en particular, $f(X)$ es irreducible en $K[X]$.

Demostración. Supongamos que existen $g, h \in R[X], g = b_0 + b_1X + \cdots + b_mX^m, h = c_0 + c_1X + \cdots + c_lX^l$ de grados positivos m y l y tales que $f = gh$ y lleguemos a una contradicción. Sea σ la proyección canónica de R a $R/(p)$ y sea σ^* el homomorfismo de anillos definido en la observación 4.2.1. La condición (i) implica que $\sigma^*(f) = \overline{a_n}X^n$, donde $\overline{a_n}$ es la clase de a_n en $R/(p)$. La condición (ii) implica que $\overline{a_n} \neq \overline{0}$ en $R/(p)$. Como R es un dominio de factorización única, (p) es un ideal primo de R, por lo que $R/(p)$ es un dominio de integridad. Como $\overline{a_n}X^n = \sigma^*(f) = \sigma^*(g)\sigma^*(h)$, se sigue del lema 4.5.1 que $\sigma^*(g)$ y $\sigma^*(h)$ son polinomios con un solo monomio cada uno. Como R es un dominio de integridad, el grado m de g y el grado l de h cumplen $m+l = n$, por lo que, necesariamente, $\sigma^*(g) = \overline{b_m}X^m$ y $\sigma^*(h) = \overline{c_l}X^l$. Esto quiere decir que p divide a $b_0, b_1, \ldots, b_{m-1}, c_0, c_1, \ldots, c_{l-1}$. De ahí se deduce que p^2 divide a $b_0c_0 = a_0$, lo cual contradice (iii). Por tanto no pueden existir $g, h \in R[X]$ de grados positivos tales que $f = gh$. Por el teorema 4.3.11, $f(X)$ es irreducible en $K[X]$. □

PARTE II: GRUPOS

Tema 5

Generalidades sobre grupos

En esta segunda parte del curso estudiaremos la noción de grupo, cuya definición (y la de grupo abeliano) vimos al principio de curso en la definición 0.1.1.

5.1 Primeras propiedades y ejemplos

Proposición 5.1.1. *Sea* $(G, *)$ *un grupo.*

(1) Existe un único elemento e *tal que* $g * e = e * g = g$ *para todo* $g \in G$.

(2) Para todo $g \in G$ *existe un único elemento* g' *tal que* $g * g' = g' * g = e$.

Demostración. La existencia de un elemento e como en (1) se tiene por la definición 0.1.1. Sean ahora $e, e' \in G$ tales que para todo $g \in G$, $g*e = e*g = g$ y $g*e' = e'*g = g$. Entonces $e = e * e' = e'$. Esto prueba (1). Dado $g \in G$, la existencia de un elemento g' como en (2) se tiene por la definición 0.1.1. Sean ahora $g', g'' \in G$ tales que $g * g' = g' * g = e$ y $g * g'' = g'' * g = e$. Entonces $g' = g' * e = g' * (g * g'') = (g' * g) * g'' = e * g'' = g''$. Esto demuestra (2). □

Notación 5.1.2. En un grupo arbitrario G llamaremos normalmente $\cdot$ a la operación de G y usaremos notación *multiplicativa*. Así, al elemento neutro del grupo $(G, \cdot)$ se le llama usualmente 1. Al inverso de un elemento $g \in G$ se le llama usualmente g^{-1}. El producto del elemento g por si mismo n veces se denota g^n y el producto de elemento g^{-1} por si mismo n veces se denota g^{-n}. Además abreviaremos $g_1 \cdot g_2$ escribiendo $g_1 g_2$ y, como $\cdot$ cumple la propiedad asociativa, prescindiremos normalmente de los paréntesis (es decir, escribiremos $g_1 g_2 g_3$ por $(g_1 g_2) g_3$ o $g_1 (g_2 g_3)$. También convenimos $g^0 = 1$.
En los ejemplos de grupos concretos sí usaremos la notación correspondiente a la operación del grupo en cuestión. Así, en los ejemplos 5.1.4 (1), (2) denotaremos por + a la operación del grupo, en los ejemplos 5.1.4 (3), (4), (5) la denotaremos por $\cdot$, en los ejemplos 5.1.5 la denotaremos por $\circ$, etc.

Observación 5.1.3. Sea G un grupo y sean $g_1, g_2 \in G$.

(1) $(g_1^{-1})^{-1} = g_1$.

(2) $(g_1g_2)^{-1} = g_2^{-1}g_1^{-1}$ ($(g_1g_2)^{-1} = g_1^{-1}g_2^{-1}$ si y solo si g_1 y g_2 conmutan; esto último ocurre por ejemplo si G es abeliano).

(3) Para todo $n \in \mathbf{Z}$, $n \neq 0$, en general $(g_1g_2)^n \neq g_1^n g_2^n$ ($(g_1g_2)^n = g_1^n g_2^n$ si g_1 y g_2 conmutan; esto último ocurre por ejemplo si G es abeliano).

Ejemplos 5.1.4. (1) Si $(R, +, \cdot)$ es un anillo (no necesariamente conmutativo ni unitario), entonces $(R, +)$ es un grupo abeliano. En $(R, +)$ no usamos la notación multiplicativa introducida en 5.1.2, sino que usaremos notación *aditiva*. Así, el elemento neutro de $(R, +)$ es 0, hablaremos de opuesto de un elemento x de R y lo denotaremos por $-x$, si $n \in \mathbf{N}$ abreviaremos $x + \overset{n)}{\cdots} + x$ como nx y abreviaremos $-x - \overset{n)}{\cdots} - x$ como $-nx$, etc.

(2) Si $(V, +, \cdot\mathbf{k})$ es un espacio vectorial, entonces $(V, +)$ es un grupo abeliano.

(3) Si $(R, +, \cdot)$ es un anillo unitario (no necesariamente conmutativo), entonces $(U(R), \cdot)$ es un grupo. Si R es conmutativo, entonces $(U(R), \cdot)$ es un grupo abeliano.

(4) Si $\mathbf{k}$ es un cuerpo, entonces $U(\mathbf{k})$ es $\mathbf{k}^* = \mathbf{k} \setminus \{0\}$, por lo que $(\mathbf{k}^*, \cdot)$ es un grupo abeliano.

(5) Si $\mathbf{k}$ es un cuerpo y $R = M_{n\times n}(\mathbf{k})$, entonces el grupo $(U(R), \cdot)$ está formado por la matrices con determinante no nulo. Este grupo se denota por $GL(n, \mathbf{k})$ (*grupo general lineal*).

Ejemplos 5.1.5. (1) Sea A un conjunto. El conjunto $\mathrm{Biy}(A)$ de las aplicaciones biyectivas de A en A con la composición de aplicaciones es un grupo, en general no abeliano.

(2) Si $A = \{1, 2, \ldots, n\}$, al grupo $(\mathrm{Biy}(A), \circ)$ se le denomina el *grupo simétrico* o el *grupo de permutaciones de n elementos* y se le denota por S_n.

Ejemplo 5.1.6. Sean $(G_1, \cdot)$ y $(G_2, \cdot)$ dos grupos. El producto cartesiano $G_1 \times G_2$ tiene estructura de grupo con respecto a la operación

$$\begin{array}{ccc} (G_1 \times G_2) \times (G_1 \times G_2) & \longrightarrow & (G_1 \times G_2) \\ ((g_1, g_2), (g_1', g_2')) & \mapsto & (g_1g_1', g_2g_2'). \end{array}$$

A $G_1 \times G_2$ se le llama *producto* de G_1 y G_2. El producto $G_1 \times G_2$ es abeliano si y solo si G_1 y G_2 son abelianos.

Observación 5.1.7. La construcción del producto de dos grupos definida en el ejemplo 5.1.6 se puede iterar de manera obvia para definir el producto de un número finito de grupos.

5.2 Subgrupos

Definición 5.2.1. Sea $(G, \cdot)$ un grupo y sea H un subconjunto no vacío de G. Decimos que H es un subgrupo de G y lo denotamos $H \leq G$ si se cumple:

(i) Para todo $h_1, h_2 \in H$ se tiene $h_1 \cdot h_2 \in H$.

(ii) Para todo $h \in H$ se tiene $h^{-1} \in H$.

Observación 5.2.2. Sea $(G, \cdot)$ un grupo y sea H un subconjunto no vacío de G. Entonces H es un subgrupo de G si y solo si para todo $h_1, h_2 \in H$, se tiene $h_1 \cdot h_2^{-1} \in H$.

Observación 5.2.3. Si H es un subgrupo de $(G, \cdot)$, es fácil ver que la operación $\cdot$ se restringe a una operación interna en H con respecto a la cual H es un grupo (en particular, si $H \leq G$, entonces $1_G \in H$). Si G es un grupo abeliano, también lo es H, aunque un subgrupo de un grupo no abeliano puede ser abeliano (considérese el ejemplo 5.2.6 (4) o cualquier subgrupo *cíclico* (véase la proposición-definición 5.4.1) de un grupo no abeliano).

Ejemplo 5.2.4. Todo grupo $(G, \cdot)$ tiene a G y a $\{1\}$ como subgrupos.

Ejemplos 5.2.5. (1) Si $(R, +, \cdot)$ es anillo e I es un ideal de R, entonces I es un subgrupo de $(R, +)$.

(2) Si $(R, +, \cdot)$ es un subanillo de $(S, +, \cdot)$, entonces R es un subgrupo de $(S, +)$.

(3) Si $(V, +, \cdot\mathbf{k})$ es un espacio vectorial y W es un subespacio vectorial de V, entonces W es un subgrupo de $(V, +)$.

(4) Si $(S, +, \cdot)$ es un anillo unitario y $(R, +, \cdot)$ es un subanillo unitario de $(S, +, \cdot)$, entonces $U(R)$ es un subgrupo de $(U(S), \cdot)$.

(5) El conjunto $\mu_n = \{\zeta \in \mathbf{C} \mid \zeta^n = 1\}$ de las raíces enésimas de la unidad es un subgrupo de $(\mathbf{C}^*, \cdot)$. En efecto, si $\zeta_1, \zeta_2 \in \mu_n$, entonces, como el producto en $\mathbf{C}^*$ es conmutativo, se tiene $(\zeta_1\zeta_2)^n = \zeta_1^n\zeta_2^n = 1$; por otra parte, si $\zeta \in \mu_n$, entonces $\zeta\zeta^{n-1} = 1$, por lo que $\zeta^{-1} = \zeta^{n-1}$ y $(\zeta^{-1})^n = (\zeta^{n-1})^n = (\zeta^n)^{n-1} = 1^{n-1} = 1$.

(6) Si S^1 es la circunferencia formada por todos los números complejos con módulo 1, entonces S^1 es un subgrupo de $(\mathbf{C}^*, \cdot)$ (para comprobarlo, usa la forma módulo-argumental o la forma exponencial de los números complejos).

Ejemplos 5.2.6. (1) Sea $(R, +, \cdot)$ un anillo. El conjunto $\mathrm{Aut}(R)$ de *automorfismos* de A (isomorfismos de anillos de A en A) es un subgrupo de $(\mathrm{Biy}(A), \circ)$.

(2) Sea V un espacio vectorial. El conjunto $\mathrm{Aut}(V)$ de los *automorfismos* de V (isomorfismos de espacios vectoriales de V en V) es un subgrupo de $(\mathrm{Biy}(V), \circ)$. El grupo $\mathrm{Aut}(V)$ también se denota como $GL(V)$ (que, como $GL(n, \mathbf{k})$ en el ejemplo 5.1.4 (5), recibe el nombre de *grupo general lineal*).

(3) Sea V un espacio vectorial euclídeo (por ejemplo, $\mathbf{R}^n$ con el producto escalar estándar). El conjunto $O(V)$ formado por las *aplicaciones ortogonales* de V (endomorfismos de V que respetan el producto escalar y que, a posteriori, son automorfismos de V) es un subgrupo de $GL(V)$. El conjunto $O^+(V)$, también denominado $SO(V)$, de las aplicaciones ortogonales de V que conservan la orientación es un subgrupo de $O(V)$. A $O(V)$ se le llama *grupo ortogonal* y a $SO(V)$ se le llama *grupo especial ortogonal*.

(4) En el caso del plano euclídeo estándar, $SO(\mathbf{R}^2)$ está formado por los giros (vectoriales) de $\mathbf{R}^2$ y $O(\mathbf{R}^2)$ está formado por los giros y las reflexiones (vectoriales) de $\mathbf{R}^2$. Recordamos, sin dar la demostración, el siguiente resultado geométrico que nos dice cómo es la composición de giros y reflexiones de $O(\mathbf{R}^2)$:

- Si g_1 es un giro (vectorial) de ángulo θ_1 y g_2 es un giro (vectorial) de ángulo θ_2, entonces $g_1 \circ g_2$ es un giro (vectorial) de ángulo $\theta_1 + \theta_2$. En particular, $g_1 \circ g_2 = g_2 \circ g_1$.
- Si r_1 es una reflexión cuyo eje es la recta (vectorial) l_1 y r_2 es una reflexión cuyo eje es la recta (vectorial) l_2, entonces $r_1 \circ r_2$ es un giro (vectorial) de ángulo -2θ, donde θ es el ángulo orientado entre l_1 y l_2. En particular $r_1 \circ r_2 \neq r_2 \circ r_1$ excepto si $r_1 = r_2$ o los ejes l_1 y l_2 son perpendiculares.
- Si g es un giro (vectorial) de ángulo θ y r es una reflexión de eje la recta (vectorial) l, entonces $g \circ r$ es una reflexión cuyo eje es la recta l girada $\theta/2$ y $r \circ g$ es una reflexión es la recta l girada $-\theta/2$. En particular $g \circ r \neq r \circ g$ excepto si g es la identidad o g es un giro de ángulo θ.

De lo anterior se deduce que, a pesar de que $O(\mathbf{R}^2)$ no es abeliano, $SO(\mathbf{R}^2)$ sí es un grupo abeliano.

(5) Sea A un espacio afín sobre un cuerpo $\mathbf{k}$ (por ejemplo, el espacio afín estándar $\mathbf{A}^n_{\mathbf{k}}$). El conjunto $\mathrm{Af}(A)$ formado por los isomorfismos afines de A en A es un subgrupo de $\mathrm{Biy}(A)$. A $\mathrm{Af}(A)$ también se le denota $GA(A)$ (*grupo general afín*).

(6) Sea A un espacio afín sobre un cuerpo $\mathbf{k}$ y sea o un punto de A. El conjunto $\mathrm{Af}(A, o)$ de isomorfismos afines de A que dejan o fijo es un subgrupo de $\mathrm{Af}(A)$.

(7) Sea A un espacio afín euclídeo (por ejemplo, el espacio afín euclídeo estándar $\mathbf{A}^n_{\mathbf{R}}$). El conjunto $\mathrm{Iso}(A)$ formado por las *isometrías* de A (aplicaciones de A en A que conservan la distancia) es un subgrupo de $\mathrm{Af}(A)$ (que a su vez es un subgrupo de $\mathrm{Biy}(A)$). El conjunto $\mathrm{Iso}^+(A)$ de isometrías de A que conservan la orientación es un subgrupo de $\mathrm{Iso}(A)$.

(8) Sea A un espacio afín euclídeo y sea o un punto de A. El conjunto de isometrías $\mathrm{Iso}(A, o)$ de A que dejan o fijo es un subgrupo de $\mathrm{Iso}(A)$ y el conjunto de isometrías $\mathrm{Iso}^+(A, o)$ de A que conservan la orientación y dejan o fijo es un subgrupo de $\mathrm{Iso}^+(A)$.

(9) Cuando $A = \mathbf{A}^2_{\mathbf{R}}$ es el plano afín euclídeo estandar, $\mathrm{Iso}(\mathbf{A}^2_{\mathbf{R}}, o)$ está formado por los giros de centro o y las reflexiones cuyo eje es una recta afín que pasa por o. La composición de dos elementos σ y τ de $\mathrm{Iso}(\mathbf{A}^2_{\mathbf{R}}, o)$ sigue las mismas reglas que la composición de sus aplicaciones lineales asociadas $\vec{\sigma}$ y $\vec{\tau}$, que son elementos de $O(\mathbf{R}^2)$.

Ejemplos 5.2.7. (1) Sea $\mathbf{k}$ cuerpo. El conjunto de matrices cuadradas de orden n con determinante 1 es un subgrupo de $GL(n, \mathbf{k})$. Se le denota $SL(n, \mathbf{k})$ (*grupo especial lineal*).

(2) El conjunto de matrices M ortogonales de orden n (aquellas matrices cuadradas reales tales que $M \cdot M^t = I_n$) es un subgrupo de $GL(n, \mathbf{R})$. Se le denota $O(n)$ y, como el caso de $O(V)$ en el ejemplo 5.2.6 (3), recibe el nombre de *grupo ortogonal*.

(3) El conjunto de matrices ortogonales de orden n y determinante 1 es un subgrupo de $O(n)$ y de $SL(n, \mathbf{R})$. Se le denota $SO(n)$ y, como el caso de $SO(V)$ en el ejemplo 5.2.6 (3), recibe el nombre de *grupo especial ortogonal*.

Observación 5.2.8. La coincidencia entre la notación de los grupos de los ejemplos 5.2.6 (2), (3) y la de los grupos de los ejemplos 5.1.4 (5) y 5.2.7 (2), (3) no es casual. Veremos en el próximo tema que, si V es un espacio vectorial sobre $\mathbf{k}$ de dimensión n, entonces $GL(V)$ y $GL(n, \mathbf{k})$ son grupos *isomorfos*. De igual manera, si V es un espacio vectorial euclídeo de dimensión n, entonces $O(V)$ y $O(n)$ son grupos isomorfos y $SO(V)$ y $SO(n)$ también son grupos isomorfos.

Como ocurre con los ideales, la intersección de subgrupos es nuevamente un subgrupo:

Proposición 5.2.9. *Sea $(G, \cdot)$ un grupo.*

(1) Si $H_1, H_2 \leq G$, entonces $H_1 \cap H_2 \leq G$.

(2) La intersección de una colección arbitraria de subgrupos de $(G, \cdot)$ es un subgrupo de $(G, \cdot)$.

Demostración. Detallamos solo la demostración de (1); la afirmación (2) es una generalización de (1) y su demostración es similar. Sean $h, h' \in H_1 \cap H_2$. Entonces $h, h' \in H_1$ y $h, h' \in H_2$. Como $H_1, H_2 \leq G$, por la observación 5.2.2 tenemos que $h \cdot (h')^{-1} \in H_1$ y $h \cdot (h')^{-1} \in H_2$, por lo que $h \cdot (h')^{-1} \in H_1 \cap H_2$. De nuevo por la observación 5.2.2, $H_1 \cap H_2 \leq G$. □

Ejemplo 5.2.10. En $GL(n, \mathbf{R})$ tenemos $SO(n) = O(n) \cap SL(n, \mathbf{R})$.

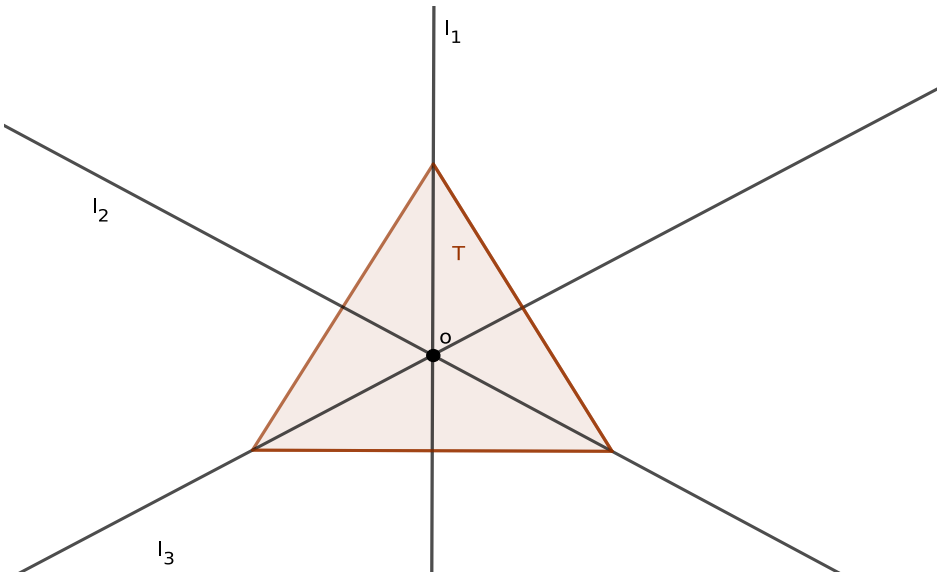
5.3 El grupo diédrico

Vemos ahora un ejemplo importante, el *grupo diédrico*.

Ejemplo 5.3.1. En el plano afín euclídeo estándar $\mathbf{A}^2_{\mathbf{R}}$ consideramos el triángulo equilátero T de la figura 5.1, con centro $o = (0,0)$ y bisectrices l_1, l_2 y l_3 Es fácil ver que las siguientes isometrías φ de $\mathbf{A}^2_{\mathbf{R}}$ dejan T invariante (es decir, cumplen $\varphi(T) = T$): la identidad (que denotaremos por id), el giro g de ángulo $2\pi/3$ y centro o, $g^2 = g \circ g$ (que es el giro de ángulo $4\pi/3$ y centro o) y las reflexiones r_1, r_2 y r_3, donde r_i es la reflexión con eje l_i. Tenemos por tanto que el conjunto $D_3 = \{\mathrm{id}, g, g^2, r_1, r_2, r_3\}$ es un subconjunto de $\mathrm{Iso}(\mathbf{A}^2_{\mathbf{R}})$ (de hecho, como todos los elementos de D_3 dejan fijo o, D_3 es un subconjunto de $\mathrm{Iso}(\mathbf{A}^2_{\mathbf{R}}, o)$). Vamos a ver que el conjunto D_3 es un subgrupo de $\mathrm{Iso}(\mathbf{A}^2_{\mathbf{R}})$ (y de $\mathrm{Iso}(\mathbf{A}^2_{\mathbf{R}}, o)$), por lo que es un grupo, que llamaremos *grupo diédrico de orden* 6. Para ello vamos a comprobar que se cumplen las propiedades (i) y (ii) de la definición 5.2.1. Para ver que se cumple (i) calculamos la composición de todas las parejas de elementos de D_3. Usando lo que se dice en los ejemplos 5.2.6 (4) y (9) es fácil ver que todas esas composiciones son de nuevo elementos de D_3. Para ver (ii) comprobamos que el inverso de todo elemento de D_3 es de nuevo un elemento de D_3. En efecto, el inverso de la identidad es la identidad, el inverso de g es g^2 (y el de g^2 es g) y el inverso de r_i es r_i.

Generalizamos a continuación el ejemplo 5.3.1:

Figura 5.1:

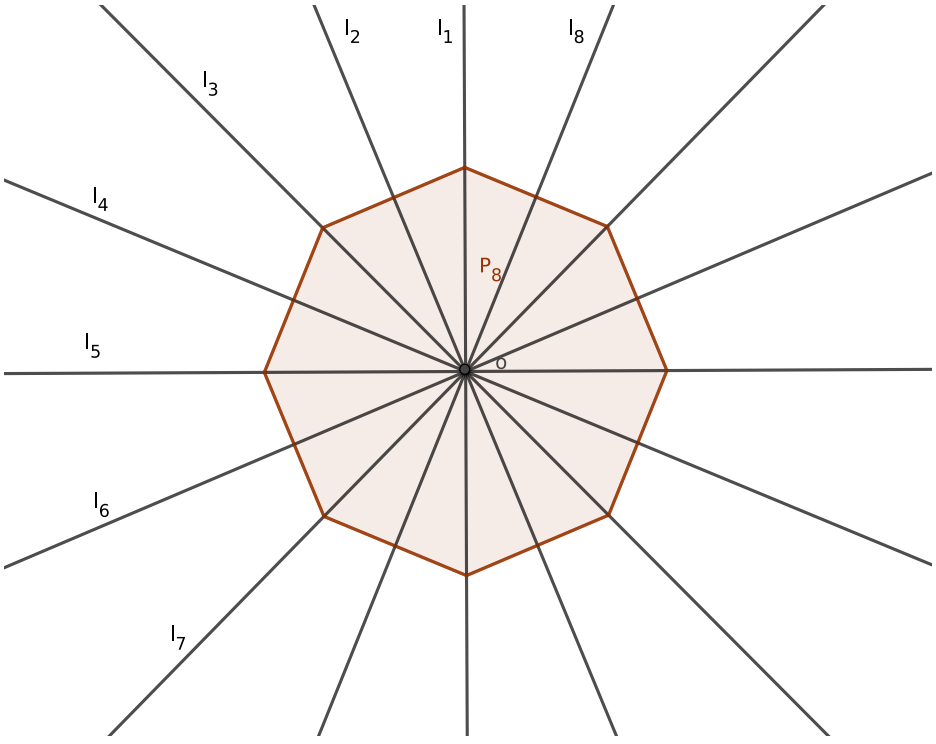


Proposición–Definición 5.3.2. *Sea $\mathbf{A}^2_{\mathbf{R}}$ el plano afín euclídeo estandar. Sea $n \geq 3$, sea P_n un polígono regular de n lados de $\mathbf{A}^2_{\mathbf{R}}$ con centro $o = (0,0)$ y con uno de sus vértices en el eje Y y sean $l_1, \ldots, l_n$ las bisectrices y mediatrices de P_n numeradas de forma consecutiva girando en sentido antihorario alrededor de o (en la figura 5.2 ilustramos la construcción para un octógono). Sea $D_n = \{id, g, g^2, \ldots, g^{n-1}, r_1, \ldots, r_n\}$, donde g es un giro de centro o y ángulo $2\pi/n$ y r_i es la reflexión de eje l_i. El conjunto D_n es un subgrupo, no abeliano, de $Iso(\mathbf{A}^2_{\mathbf{R}})$ (y de $Iso(\mathbf{A}^2_{\mathbf{R}}, o)$) y recibe el nombre de* grupo diédrico de orden $2n$.

Demostración. La demostración sigue los mismos argumentos del ejemplo 5.3.1 y la dejamos como ejercicio. □

Es claro que los elementos del conjunto $\{\mathrm{id}, g, g^2, \ldots, g^{n-1}, r_1, \ldots, r_n\}$ son isometrías de $\mathbf{A}^2_{\mathbf{R}}$ que dejan P_n invariante. En realidad son las únicas, como nos asegura la proposición 5.3.3. Aunque la proposición 5.3.3 se puede probar usando razonamientos geométricos elementales, no incluimos una demostración aquí; sí daremos una demostración en el tema

Figura 5.2:



8 (corolario 8.3.5), que usa algunos de esos razonamientos y el concepto de *acción* de un grupo sobre un conjunto.

Proposición 5.3.3. *Los isomorfismos afines del plano afín euclídeo estándar $\mathbf{A}^2_{\mathbf{R}}$ que dejan P_n invariante son necesariamente isometrías de $\mathbf{A}^2_{\mathbf{R}}$ y son exactamente las isometrías $id, g, g^2, \ldots, g^{n-1}$, $r_1, \ldots, r_n$ descritas en la proposición–definición 5.3.2.*

Observación 5.3.4. La proposición 5.3.3 se puede extender a cualquier polígono regular P'_n de n lados en $\mathbf{A}^2_{\mathbf{R}}$. En efecto, el conjunto de isometrías que dejan P'_n invariante está formado por giros con centro el centro de P'_n y reflexiones con ejes las bisectrices y mediatrices de P'_n, por lo que, en general, dicho conjunto será distinto de $\{\mathrm{id}, g, g^2, \ldots, g^{n-1}, r_1, \ldots, r_n\}$. Aun así, el conjunto de isometrías que dejan P'_n invariante es un grupo *isomorfo* a $\{\mathrm{id}, g, g^2, \ldots, g^{n-1}, r_1, \ldots, r_n\}$; de hecho, ambos grupos son subgrupos *conjugados* en $\mathrm{Iso}(\mathbf{A}^2_{\mathbf{R}})$ (el concepto de grupos isomorfos y el de subgrupos conjugados los veremos en el próximo tema). Por tanto, a cualquiera de estos grupos isomorfos entre sí lo podríamos llamar grupo diédrico D_n. De hecho, D_n es más bien un grupo "abstracto" con $2n$ elementos cuya tabla es la misma que la del grupo $\{\mathrm{id}, g, g^2, \ldots, g^{n-1}, r_1, \ldots, r_n\}$ con la composición (por ello ese grupo abstracto y $\{\mathrm{id}, g, g^2, \ldots, g^{n-1}, r_1, \ldots, r_n\}$ serán isomorfos). Desde ese punto de vista el grupo de isometrías de un polígono regular de n lados es un modelo concreto de D_n.

Observación 5.3.5. La proposición 5.3.3 nos da otra forma de ver que

$$\{\mathrm{id}, g, g^2, \ldots, g^{n-1}, r_1, \ldots, r_n\}$$

es un subgrupo de $\mathrm{Iso}(\mathbf{A}^2_{\mathbf{R}})$ ya que, si D_n son las isometrías de $\mathbf{A}^2_{\mathbf{R}}$ que dejan P_n invariante, es claro que la composición de dos isometrías que dejan P_n invariante es una isometría que deja P_n invariante y la aplicación inversa de una isometría que deja P_n invariante es una isometría que deja P_n invariante.

5.4 Grupos cíclicos

Una clase importante de grupos es la de aquellos *generados* por un solo elemento:

Proposición–Definición 5.4.1. *Sea G un grupo y sea $g \in G$.*

(1) El conjunto $\{g^n \mid n \in \mathbf{Z}\}$ es un subgrupo de G, que se llama subgrupo cíclico generado por g y se denota $<g>$.

(2) Decimos que G es un grupo cíclico generado por g si $G = <g>$.

(3) Los grupos cíclicos son abelianos.

Demostración. Vemos que $<g>$ es un subgrupo. Dados $n, m \in \mathbf{Z}$, según la notación 5.1.2, $g^n g^m = g^{n+m}$, que pertenece a $< g >$, por lo que se cumple la propiedad (i) de la definición 5.2.1. Como la suma en $\mathbf{Z}$ es conmutativa, esto demuestra también que la operación de G es conmutativa al restringirla a $<g>$. Por otra parte, si $n \in \mathbf{N}$, entonces $(g^n)^{-1} = (g \overset{n)}{\cdots} \cdot g)^{-1} = g^{-1} \overset{n)}{\cdots} \cdot g^{-1} = g^{-n}$ pertenece a $<g>$. Si $n \in \mathbf{Z}$ y $n < 0$, entonces $(g^n)^{-1} = (g^{-1} \overset{-n)}{\cdots} \cdot g^{-1})^{-1} = g \overset{-n)}{\cdots} \cdot g = g^{-n}$ pertenece a $< g >$. Finalmente $g^0 = 1$ y su inverso es $1 = g^0$, que pertenece a $< g >$. Así pues se cumple la propiedad (ii) de la definición 5.2.1. □

Definición 5.4.2. Sea G un grupo y sea $g \in G$.

(1) Si G es un grupo finito, al cardinal de G se le llama *orden* de G.

(2) Si $<g>$ es finito, se llama *orden* de g al orden de $<g>$.

Ejemplos 5.4.3. (1) El orden de S_n es $n!$.

(2) El orden de D_n es $2n$.

(3) El orden de $(\mathbf{Z}_n, +)$ es n.

(4) El orden de $(\mu_n, \cdot)$ es n.

Recordamos la siguiente definición introducida en el ejercicio 23 del tema 3:

Definición 5.4.4. Sea

$$\begin{array}{rccc} \varphi: & \mathbf{N} \setminus \{1\} & \longrightarrow & \mathbf{N} \\ & n & \mapsto & \varphi(n), \end{array}$$

la aplicación tal que $\varphi(n)$ es el cardinal del conjunto formado por los números naturales menores que n tales que 1 es máximo común divisor de m y n. A φ se le denomina la *función de Euler*.

Ejemplo 5.4.5. Según vimos en el ejercicio 23 del tema 3, para $n > 1$, el orden del grupo de unidades $(U(\mathbf{Z}_n), \cdot)$ de $(\mathbf{Z}_n, +, \cdot)$ es $\varphi(n)$.

Proposición 5.4.6. *Sea G un grupo y sea $g \in G$. El subgrupo $<g>$ es finito si y solo si $g^m = 1$ para algún $m \in \mathbf{N}$. En ese caso el orden de g es el menor número natural n tal que $g^n = 1$ y $<g> = \{1, g, g^2, \ldots, g^{n-1}\}$.*

Demostración. Supongamos que $<g>$ es finito. En ese caso la aplicación

$$\begin{array}{ccc} \mathbf{N} & \longrightarrow & <g> \\ n & \mapsto & g^n \end{array}$$

no es inyectiva, por lo que existen dos números naturales m_1 y m_2 distintos tales que $g^{m_1} = g^{m_2}$. Supongamos que, por ejemplo, $m_2 > m_1$. Entonces tomando $m = m_2 - m_1$, tenemos que $m \in \mathbf{N}$ y $g^m = 1$.

Supongamos ahora que existe $m \in \mathbf{N}$ tal que $g^m = 1$. Sea n el número natural más pequeño con esa propiedad. Sea ahora $s \in \mathbf{Z}$, sean $q, r \in \mathbf{Z}$, respectivamente, el cociente y el resto, entre 0 y $n-1$, de dividir s entre n. Entonces, según (5.1.2), $g^s = g^{nq+r} = (g^n)^q g^r = g^r$, por lo que todo elemento de $<g>$ es igual a un elemento del conjunto $\{1, g, \ldots, g^{n-1}\}$. Por otra parte, si r_1, r_2 son enteros no negativos distintos y menores que n, entonces $g^{r_1} \neq g^{r_2}$ pues, en caso contrario, si, por ejemplo, $r_2 > r_1$, se tendría $g^{r_2-r_1} = 1$. Sin embargo $r_2 - r_1 \leq r_2 < n$, y esto contradiría la minimalidad de n. Por tanto $<g> = \{1, g, g^2, \ldots, g^{n-1}\}$ tiene n elementos. □

Observación 5.4.7. Si G es un grupo finito de orden n, G es un grupo cíclico generado por g si y solo si el orden de g es n.

Corolario 5.4.8. *Sea G un grupo y sea $g \in G$. Si $n \in \mathbf{N}$ es el orden de g, e entonces un número entero m cumple $g^m = 1$ si y solo si n divide a m.*

Demostración. Si existe $m' \in \mathbf{Z}$ tal que $m = m'n$, entonces $g^m = g^{m'n} = (g^n)^{m'} = 1^{m'} = 1$, ya que $g^n = 1$ por la proposición 5.4.6.
Sea ahora $m \in \mathbf{Z}$ tal que $g^m = 1$. Sean $q, r \in \mathbf{Z}$, respectivamente, el cociente y el resto, entre 0 y $n-1$, de dividir m entre n. Argumentando como en la demostración de la proposición 5.4.6 vemos que $1 = g^m = g^r$. Por la minimalidad de n, tenemos entonces que $r = 0$, por lo que $m = qn$. □

Ejemplos 5.4.9. (1) Sea G un grupo. El orden de 1 es 1.

(2) El grupo trivial de un solo elemento $G = \{1\}$ es obviamente cíclico de orden 1.

(3) Un grupo $G = \{1, g\}$ de dos elementos es cíclico de orden 2 ya que, como $g \neq 1$, necesariamente $g^2 = 1$. Por tanto $G = <g>$.

Ejemplo 5.4.10. (1) El grupo $(\mathbf{Z}, +)$ es cíclico infinito y sus generadores son únicamente 1 y -1.

(2) En general, si $G = <g>$ es un grupo cíclico infinito, entonces sus únicos generadores son g y g^{-1}. En efecto, si g^s es un generador de G, entonces existe $t \in \mathbf{Z}$ tal que $g = (g^s)^t = g^{st}$, por lo que $g^{st-1} = g^{1-st} = 1$. Como G es cíclico infinito, de la proposición 5.4.6 se sigue que ninguno de los dos números enteros $st - 1$ y $1 - st$ son números naturales, por lo que $st - 1 = 1 - st = 0$, de donde $st = 1$ y $s = \pm 1$.

Ejemplo 5.4.11. Sea G es un grupo cíclico de orden n y sea g un generador de G. Si $s \in \mathbf{Z}$, entonces el orden de g^s es $\frac{n}{\text{m.c.d.}(s,n)}$, donde tomamos m.c.d.$(s, n)$ en $\mathbf{N}$. En particular, los generadores de G son los elementos g^r, donde $r \in \mathbf{Z}$, $r \neq 0$ y m.c.d.$(r, n) = 1$. El número de generadores de G es por tanto $\varphi(n)$, donde φ es la función de Euler definida en la definición 5.4.4.
En efecto, consideramos el número natural $d = \text{m.c.d.}(s, n)$ y sean $s' \in \mathbf{Z}$ y $n' \in \mathbf{N}$ tales que $s = s'd$ y $n = n'd$ (por tanto, $n' = \frac{n}{\text{m.c.d.}(s,n)}$). Entonces $(g^s)^{n'} = g^{s'n'd} = (g^n)^{s'} = 1$.

Por otra parte sea $m \in \mathbf{N}$ tal que $(g^s)^m = 1$. Entonces $g^{ms} = 1$ y, por el corolario 5.4.8, n divide a ms. Entonces existe $l \in \mathbf{Z}$ tal que $ms'd = ms = ln = ln'd$, de donde $ms' = ln'$. Como s' y n' son primos entre sí, de la unicidad de la descomposición de un número natural como producto de primos se sigue que n' divide a m y, en particular, $n' \leq m$. Por tanto, la proposición 5.4.6 nos dice que $n' = \frac{n}{\text{m.c.d.}(s,n)}$ es el orden de g^s.

Ejemplos 5.4.12. Los siguientes son ejemplos de grupos cíclicos finitos de orden n:

(1) El grupo $(\mathbf{Z}_n, +)$, que está generado por $\overline{1}$. Por el ejemplo 5.4.11, dado $\overline{r} \in \mathbf{Z}_n$, el orden de $\overline{r}$ es $\frac{n}{\text{m.c.d.}(r,n)}$ y los generadores de $(\mathbf{Z}_n, +)$ son los elementos $\overline{r}$ de $\mathbf{Z}_n$ tales que n y r son primos entre sí. Por ejemplo, los generadores de $(\mathbf{Z}_{12)}, +)$ son $\overline{1}$, $\overline{5}$, $\overline{7}$ y $\overline{11}$.

(2) Análogamente a (1), el grupo $(\mathbf{Z}/(n), +)$, es cíclico de orden n y está generado por $\overline{1}$. Por el ejemplo 5.4.11, dado $\overline{s} \in \mathbf{Z}/(n)$, el orden de $\overline{s}$ es $\frac{n}{\text{m.c.d.}(s,n)}$ y los generadores de $(\mathbf{Z}/(n), +)$ son los elementos $\overline{s}$ de $\mathbf{Z}/(s)$ tales que n y s son primos entre sí.

(3) El grupo $(\mu_n, \cdot)$, que está generado el número complejo de módulo 1 y argumento $\frac{2\pi}{n}$. Según el ejemplo 5.4.11 todos sus generadores son los números complejos de módulo 1 y argumento $\frac{2r\pi}{n}$ con $s \in \mathbf{N}$ tal que r y n son primos entre sí. A los generadores de $(\mu_n, \cdot)$ se les denomina *raíces primitivas enésimas de la unidad*.

Además, si ζ tiene módulo 1 y argumento $\frac{2s\pi}{n}$, con $s \in \mathbf{N}$, entonces el orden de ζ es $\frac{n}{\text{m.c.d.}(s,n)}$.

Ejemplo 5.4.13. Sea $v \in \mathbf{R} \setminus \mathbf{Q}$ y sea z el número complejo de módulo 1 y argumento $2v\pi i$. Según la proposición 5.4.6, el subgrupo $< z >$ de $(\mathbf{C}^*, \cdot)$ es cíclico infinito. Según el ejemplo 5.4.10 (2), los únicos generadores de $< z >$ son z y z^{-1}, que es el número complejo de módulo 1 y argumento $-2v\pi i$.

Ejemplo 5.4.14. El grupo diédrico (véase la proposición-definición 5.3.2) D_n $(n \geq 3)$ no es cíclico ya que no es abeliano. El subgrupo $< g >$ de D_n es cíclico de orden n y sus genereradores son los giros g^m distintos de la identidad tales que $\text{mcd}(m,n) = 1$. El orden de g^m es $\frac{n}{\text{m.c.d.}(m,n)}$. Los subgrupos $<r_i>$ son cíclicos de orden 2.

Ejemplo 5.4.15. El grupo $(\mathbf{Z}_5^*, \cdot)$ de las unidades del cuerpo $\mathbf{Z}_5$ es cíclico de orden 4. Sus generadores son $\overline{2}$ y $\overline{3}$. El orden de $\overline{1}$ es 1 y el orden de $\overline{4}$ es 2. En el último tema veremos que el grupo de unidades de un cuerpo finito es cíclico.

Observación 5.4.16. En el tema siguiente veremos que todos los grupos cíclicos infinitos son *isomorfos* entre sí y que, dado $n \in \mathbf{N}$, todos los grupos cíclicos de orden n son *isomorfos* entre sí. En particular el grupo G del ejemplo 5.4.10 (2), el grupo $(\mathbf{Z}, +)$ y el grupo $< z >$ del ejemplo 5.4.13 son grupos isomorfos. Asimismo los grupos $(\mathbf{Z}_n, +)$, $(\mathbf{Z}/(n), +)$, $(\mu_n, \cdot)$

y el subgrupo $< g >$ de D_n del ejemplo 5.4.14 son grupos isomorfos. De igual forma, $(\mathbf{Z}_4, +)$ y $(\mathbf{Z}_5^*, \cdot)$ son grupos isomorfos. Esto justifica que, tal y como hemos visto en los ejemplos anteriores, los grupos cíclicos infinitos se comporten igual en lo que se refiere a sus generadores y los grupos cíclicos de orden finito n se comporten igual en lo que se refiere a sus generadores y al orden de sus elementos.

Un grupo cíclico está generado por un elemento, pero, como demuestra el ejemplo 5.4.14, no todos los grupos son cíclicos. Una noción más general que la de grupo cíclico sería la de grupo *finitamente generado*, que introducimos a continuación:

Proposición–Definición 5.4.17. *Sea G un grupo.*

(1) Sea $\Sigma \subseteq G$. El conjunto formado por todos los productos finitos de elementos de Σ, es decir, por las expresiones $a_{i_1} a_{i_2} \cdots a_{i_s}$, donde $a_{i_1}, a_{i_2}, \ldots, a_{i_s}$ son elementos, no necesariamente distintos, de Σ, es un subgrupo de G. A este subgrupo le llamamos el subgrupo generado *por Σ y lo denotamos como $< \Sigma >$. En el caso de que Σ sea un conjunto finito $\{a_1, a_2, \ldots, a_k\}$, escribimos $<a_1, a_2, \ldots, a_k>$ en vez de $<\Sigma>$.*

(2) Decimos que G está finitamente generado *si existen elementos $a_1, a_2, \ldots, a_k$ de G tales que $G = <a_1, a_2, \ldots, a_k>$. Decimos que $a_1, a_2, \ldots, a_k$ es un conjunto de* generadores *de G.*

Demostración. Lo único que hay que demostrar es que $< \Sigma >$ es un subgrupo de G. Lo dejamos como un sencillo ejercicio. □

Proposición 5.4.18. *Sea G un grupo y sea $\Sigma \subseteq G$.*

(1) El subgrupo $< \Sigma >$ es la intersección de todos los subgrupos de G que contienen a Σ.

(2) El subgrupo $< \Sigma >$ es el "subgrupo más pequeño" que contiene a Σ, es decir, es el único subgrupo H de G que cumple

(i) $\Sigma \subseteq H$; y

(ii) para todo $H' \leq G$ tal que $\Sigma \subseteq H'$ se tiene $H \subseteq H'$.

Demostración. La intersección de todos los subgrupos de G que contienen a Σ es un subgrupo de G. Por lo demás, la demostración del resultado es análoga a las demostraciones de las proposiciones 2.1.13 y 2.1.14, por lo que la dejamos como ejercicio. □

Aunque los grupos finitamente generados son más generales que los grupos cíclicos, no todos los grupos son finitamente generados. Por ejemplo, como veremos en el tema 9, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ y $(\mathbf{C}, +)$ no son grupos finitamente generados.

5.5 Índice de un subgrupo

Proposición–Definición 5.5.1. *Sea H un subgrupo de $(G, \cdot)$. Entonces H define dos relaciones de equivalencia en G, que denotamos R_H y R^H, de la siguiente forma:*

(1) $g_1 R_H g_2$ *si y solo si* $g_1 g_2^{-1} \in H$.

(2) $g_1 R^H g_2$ *si y solo si* $g_1^{-1} g_2 \in H$.

La clase de equivalencia de g respecto de R_H es $Hg := \{hg \mid h \in H\}$ y la clase de equivalencia de g respecto de R^H es $gH := \{gh \mid h \in H\}$.

Al conjunto cociente de G por la relación R_H lo denotamos G/R_H y al conjunto cociente de G por la relación R^H lo denotamos G/R^H, como es costumbre.

Demostración. Demostramos que R_H es una relación de equivalencia (la demostración para R^H es análoga). La relación R_H es reflexiva, ya que para todo $g \in G$, $gg^{-1} = 1 \in H$. Es simétrica, ya que si $g_1 R_H g_2$, entonces $g_1 g_2^{-1} \in H$ y, como H es un subgrupo, se tiene $g_2 g_1^{-1} = (g_1 g_2^{-1})^{-1} \in H$, por lo que $g_2 R_H g_1$. Finalmente, es transitiva, ya que si $g_1 R_H g_2$ y $g_2 R_H g_3$, entonces $g_1 g_2^{-1} \in H$ y $g_2 g_3^{-1} \in H$ y, como H es un subgrupo, $g_1 g_3^{-1} = g_1 \cdot 1 \cdot g_3^{-1} = g_1 (g_2^{-1} g_2) g_3^{-1} = (g_1 g_2^{-1})(g_2 g_3^{-1}) \in H$.

Vemos ahora cómo son las clases de equivalencia respecto de R_H (cómo son las clases de equivalencia respecto de R^H se ve de manera análoga). Si $g \in H$, la clase de equivalencia de g respecto de R_H es el conjunto $\{g' \mid g' R_H g\} = \{g' \mid g' g^{-1}$ pertenece a $H\} = \{g' \mid$ existe h en H tal que $h = g' g^{-1}\} = \{hg \mid h \in H\}$. □

Observación 5.5.2. En general, las relaciones R_H y R^H son distintas, ya que si $g_1 R_H g_2$, entonces $g_2 g_1^{-1} \in H$ pero esto no tiene por qué implicar que $g_1^{-1} g_2 \in H$, es decir, no tiene por qué implicar que $g_1 R^H g_2$, si G no es abeliano, tal como nos muestra el ejemplo 5.5.4. Veremos más adelante que cuando H es un *subgrupo normal*, las relaciones R_H y R^H sí coinciden.

Observación 5.5.3. Según se mencionó en el ejemplo 5.2.5 (1), un ideal I de un anillo $(R, +, \cdot)$ es un subgrupo del grupo abeliano $(R, +)$. Por lo dicho en la observación 5.5.2, las dos relaciones de equivalencia definidas por el subgrupo I en el grupo $(R, +)$ coinciden. De hecho son la relación de equivalencia definida en la proposición 2.2.1 por el ideal I en el anillo $(R, +, \cdot)$.

Ejemplo 5.5.4. Sean $G = D_3$ y $H = \{\mathrm{id}, r_1\}$, que, obviamente, es un subgrupo de G. Si R_H y R^H fueran la misma relación de equivalencia, las clases de equivalencia de un elemento respecto R_H y a R^H serían las mismas. Sin embargo, $Hg = \{g, r_3\}$ y $gH = \{g, r_2\}$.

Proposición 5.5.5. *(1) Las aplicaciones*

$$\begin{array}{ccc} H & \longrightarrow & Hg \\ h & \mapsto & hg, \end{array}$$

$$\begin{array}{ccc} H & \longrightarrow & gH \\ h & \mapsto & gh \end{array}$$

son aplicaciones biyectivas.

(2) La aplicación

$$\begin{array}{ccc} G/R^H & \longrightarrow & G/R_H \\ gH & \mapsto & Hg^{-1} \end{array}$$

está bien definida y es biyectiva.

Demostración. Vemos que la primera de las aplicaciones es biyectiva (el razonamiento para la segunda es análogo). Si $h_1, h_2 \in H$ y $h_1 g = h_2 g$, entonces $(h_1 g)g^{-1} = (h_2 g)g^{-1}$, por lo que $h_1(gg^{-1}) = h_2(gg^{-1})$ y $h_1 = h_2$. Esto prueba que la aplicación es inyectiva. Por otra parte, si $g' \in Hg$, existe $h \in H$ tal que $g' = hg$, por lo que la aplicación envía h a g'. Esto prueba que la aplicación es sobreyectiva.

Vemos ahora que la aplicación entre los conjuntos cocientes está bien definida. Sean $g_1H, g_2H \in G/R^H$ tales que $g_1H = g_2H$. Esto quiere decir que $g_1 R^H g_2$, es decir, que $g_1^{-1}g_2 \in H$. Veamos que $g_1^{-1} R_H g_2^{-1}$, de donde obtendremos que $Hg_1^{-1} = Hg_2^{-1}$. Pero es claro que $g_1^{-1} R_H g_2^{-1}$ ya que $g_1^{-1}(g_2^{-1})^{-1} = g_1^{-1}g_2 \in H$. Vemos ahora que la aplicación es biyectiva. Sean $g_1H, g_2H \in G/R^H$ y supongamos que $Hg_1^{-1} = Hg_2^{-1}$. Entonces $g_1^{-1} R_H g_2^{-1}$, es decir, $g_1^{-1}(g_2^{-1})^{-1} = g_1^{-1}g_2$ pertenece a H, por lo que $g_1 R^H g_2$ y $g_1H = g_2H$. Esto demuestra que la aplicación es inyectiva. Finalmente, sea $Hg' \in G/R_H$. Entonces $g'^{-1}H$, que es un elemento de G/R^H, se aplica en Hg', por lo que la aplicación es sobreyectiva. □

Definición 5.5.6. Sea G un grupo y sea H un subgrupo de G. Si G/R_H es un conjunto finito (observa que esto no implica necesariamente que G sea finito, veáse el ejemplo 5.5.8(3)) entonces al cardinal de G/R_H (que es el mismo que el de G/R^H por la proposición 5.5.5) se le llama *índice* de H en G y se denota $[G : H]$.

Observación 5.5.7. Sea G un grupo y sea H un subgrupo de G de orden finito m. Se sigue de la proposición 5.5.5 que las clases de equivalencia respecto de R_H y de R^H tienen todas el mismo número de elementos y este es igual a m.

Ejemplos 5.5.8. (1) Sea $G = D_3$ y sea $H = \{\mathrm{id}, r_1\}$. En ese caso el orden de H es 2. Por otra parte $H\mathrm{id} = \{\mathrm{id}, r_1\}$, $Hg = \{g, r_3\}$ y $Hg^2 = \{g^2, r_2\}$, por lo que $G/R_H = \{H\mathrm{id}, Hg, Hg^2\}$. Por tanto $[G : H] = 3$.

(2) Sea $G = D_3$ y sea $H' = \{id, g, g^2\}$, que es un subgrupo de G. En ese caso el orden de H' es 3. Por otra parte $H\mathrm{id} = \{\mathrm{id}, g, g^2\}$ y $Hr_1 = \{r_1, r_2, r_3\}$, por lo que $G/R_{H'} = \{H\mathrm{id}, Hr_1\}$. Por tanto $[G : H'] = 2$.

(3) Sea $G = O(n)$ y sea $H = SO(n)$. Aunque G es infinito, $[G : H] = 2$ ya que G/R_H consta de solo dos elementos, que son la clase de I_n y la clase de J_n, donde J_n es la matriz diagonal que tiene 1 en todas las entradas de la diagonal excepto en la última, que es -1. En efecto, para comprobar esto basta ver que I_n y J_n no están relacionadas, con lo que sus clases HI_n y HJ_n serán distintas, y que cualquier matriz M de $O(n)$ está relacionada con I_n o con J_n, con lo que HI_n y HJ_n serán las únicas clases de G/R_H. Que I_n y J_n no están relacionados es claro, ya que $\det(I_nJ_n^{-1})=\det(I_n)\det(J_n)^{-1} = -1$, así que $I_nJ_n^{-1} \notin SO(n)$. Sea ahora $M \in O(n)$. Veamos que si M no está relacionada con I_n, lo está con J_n. Si M no está relacionada con I_n, quiere decir que $MI_n^{-1} \notin SO(n)$, es decir, que $\det(M)=\det(MI_n^{-1}) \neq 1$. En ese caso $\det M = -1$, por lo que $\det(MJ_n^{-1}) =\det(M)\det(J_n^{-1}) = (-1)(-1) = 1$, de donde $MJ_n^{-1} \in SO(n)$ y M está relacionada con J_n.

Teorema 5.5.9. (Lagrange). *Sea G un grupo finito de orden n y sea H un subgrupo de G de orden m. Entonces $n = [G : H] \cdot m$. En particular, m divide a n.*

Demostración. La relación de equivalencia R_H proporciona una partición de G de manera que G se escribe como unión disjunta de las clases de equivalencia de R_H. Según la observación 5.5.7 todas las clases de equivalencia de R_H tienen m elementos. Por otra parte el índice $[G : H]$ de H en G es el cardinal del conjunto cociente G/R_H, por lo que el cardinal, es decir, el orden de G, es el producto de $[G : H]$ y m. □

Corolario 5.5.10. *Sea G un grupo finito de orden n, sea $g \in G$ y sea k el orden de g. Entonces*

(1) se cumple que k divide a n;

(2) se cumple $g^n = 1$.

Demostración. Como k es el orden de $< g >$, la afirmación (1) es un caso particular del teorema 5.5.9. Sea $g \in G$ y sea k el orden de g. Entonces existe $l \in \mathbf{N}$ tal que $n = kl$, por lo que $g^n = g^{kl} = (g^k)^l = 1^l = 1$. □

Corolario 5.5.11. *Sea p un número primo. Si G es un grupo de orden p, entonces G es cíclico y todo $g \in G, g \neq 1$ es un generador de G.*

Demostración. Sea $g \in G$, $g \neq 1$. En ese caso el orden de g es mayor que 1 y, por el teorema 5.5.9, divide a p, por lo que el orden de g ha de ser p y, por la observación 5.4.7, $G =< g >$. □

Ejemplo 5.5.12. Usamos la notación de la proposición-definición 5.3.2.

(a) El grupo diédrico D_n está generado por el giro g y por una cualquiera de sus reflexiones. En efecto, según el ejemplo 5.4.14, el subgrupo $< g >$ tiene orden n. El orden de $< g, r_i >$ es mayor que n, ya que $r_i \notin < g >$. Como D_n tiene orden $2n$, el teorema 5.5.9 implica $< g, r_i >= D_n$.

(b) De igual forma, si $m \in \mathbf{N}$, $m < n$ y m.c.d$(m, n) = 1$, se sigue también del ejemplo 5.4.14 que D_n está generado por g^m y una reflexión cualquiera de D_n.

(c) Además, para todo $i \in \mathbf{N}$, $i \leq n-1$, el grupo D_n está generado por r_i y r_{i+1}, ya que $r_{i+1} \circ r_i = g$. De igual forma D_n está generado por r_1 y r_n.

Observación 5.5.13. El teorema 5.5.9 nos dice que si G es un grupo de orden n y m es un número natural que no divide a n, entonces G no tiene ningún subgrupo de orden m ni ningún elemento de orden m. Por ejemplo, S_5, que tiene orden 120, no tiene ningún subgrupo ni ningún elemento de orden 7 ni ningún subgrupo ni ningún elemento de orden 14. Sin embargo, el teorema 5.5.9 no nos dice que si $m \in \mathbf{N}$ divide a n, entonces G tenga necesariamente subgrupos y elementos de orden m. Por ejemplo, veremos en el tema 8 que S_5 no tiene subgrupos de orden 30 ni de orden 40 (véase el ejercicio 9 del tema 8) a pesar de que 30 y 40 dividen a 120. Asimismo veremos en el tema 7 que S_5 no tiene elementos de orden 30 ni de orden 40. Por tanto, el recíproco del teorema de Lagrange no es cierto (véase también el ejercicio 12 del tema 7).

Ejemplos 5.5.14. (1) El grupo $(\mathbf{Z}_2 \times \mathbf{Z}_2, +)$ tiene orden 4 pero todos sus elementos distintos del neutro tienen orden 2. En particular, $(\mathbf{Z}_2 \times \mathbf{Z}_2, +)$ no es cíclico. En general, dado $n \in \mathbf{N}$, los elementos de $G = (\mathbf{Z}_2 \times \overset{n)}{\cdots} \times \mathbf{Z}_2, +)$ distintos del neutro tienen todos orden 2, por lo que si $n > 1$, G no es cíclico y es otro ejemplo de que, en lo que respecta al orden de un elemento, el recíproco del teorema de Lagrange no es cierto.

(2) Los posibles órdenes para los elementos y para los subgrupos de D_3 son $1, 2, 3$ y 6. Los elementos de D_3 tienen estos órdenes: la identidad tiene orden 1, r_1, r_2 y r_3 tienen orden 2 y g y g^2 tienen orden 3. Por tanto, no existe ningún elemento de D_3 de orden 6, por lo que D_3 no es cíclico (ya lo sabíamos porque D_3 no es abeliano). En cuanto a sus subgrupos, D_3 tiene subgrupos de todos los órdenes posibles. En efecto, <id> es el único subgrupo de orden 1 y D_3 es el único subgrupo de orden 6. Los subgrupos de orden 2 han de ser cíclicos, porque 2 es primo, por lo tanto los subgrupos de orden 2 de D_3 son $<r_1>, <r_2>$ y $<r_3>$. Igualmente, como 3 es primo, los subgrupos de D_3 de orden 3 son cíclicos, por lo que solo hay un subgrupo de orden 3, que es $<g>$ ya que $<g>=<g^2>$.

Finalizamos este tema con una aplicación del teorema 5.5.9 a las congruencias:

Corolario 5.5.15. *(teorema de Euler). Si a y n son números enteros primos entre sí, entonces*

$$a^{\varphi(n)} \equiv 1 \text{ mód } n, \tag{5.5.15.1}$$

donde φ es la función de Euler introducida en la definición 5.4.4.

Demostración. Según la observación 3.5.2, la congruencia (5.5.15.1) es equivalente a

$$\overline{a}^{\varphi(n)} = \overline{1} \tag{5.5.15.2}$$

en $\mathbf{Z}/(n)$. Según el corolario 3.4.9, como a y n son primos entre sí, $\overline{a}$ es una unidad del anillo $\mathbf{Z}/(n)$, es decir, $\overline{a}$ es un elemento del grupo $(U(\mathbf{Z}/(n)), \cdot)$. Como, por el ejemplo 5.4.5, el grupo $(U(\mathbf{Z}/(n)), \cdot)$ tiene orden $\varphi(n)$, la igualdad (5.5.15.2) se sigue del corolario 5.5.10 (2). □

Corolario 5.5.16. *(pequeño teorema de Fermat). Si p es un número primo, entonces, para todo número entero a se cumple*

$$a^p \equiv a \text{ mód } p. \tag{5.5.16.1}$$

Demostración. Si a es múltiplo de p, entonces $a \equiv 0$ mód p y $a^p \equiv 0$ mód p, por lo que (5.5.16.1) se cumple en ese caso.

Si a no es múltiplo de p, como p es primo, se sigue que a y p son primos entre sí. Por otra parte, como p es primo, $\varphi(p) = p - 1$. Entonces el corolario 5.5.15 nos dice que

$$a^{p-1} \equiv 1 \text{ mód } p \tag{5.5.16.2}$$

y, multiplicando (5.5.16.2) por a en ambos miembros obtenemos (5.5.16.1) en este caso. □

Tema 6

Homomorfismos de grupos. Subgrupos normales

6.1 Homomorfismos de grupos

Definición 6.1.1. Sean $(G, *)$ y $(G', \cdot)$ dos grupos y sea $\varphi : G \longrightarrow G'$ una aplicación. Decimos que φ es un homomorfismo de grupos si para cualesquiera $g_1, g_2 \in G$ se tiene que $\varphi(g_1 * g_2) = \varphi(g_1) \cdot \varphi(g_2)$.

Proposición 6.1.2. *Sean $\varphi : G \longrightarrow G'$ un homomorfismo de grupos. Entonces*

(1) $\varphi(1_G) = 1_{G'}$.

(2) Para todo $g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Demostración. Sea $\varphi(1_G) = g'$. Entonces $g' = \varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \cdot \varphi(1_G) = g'^2$. Multiplicando la igualdad anterior por g'^{-1}, obtenemos $g' = 1_{G'}$. Por otra parte $1_{G'} = \varphi(1_G) = \varphi(g * g^{-1}) = \varphi(g) \cdot \varphi(g^{-1})$ por lo que $\varphi(g^{-1})$ es, en efecto, el inverso de $\varphi(g)$. □

Ejemplos 6.1.3. (1) Si G es un grupo, la aplicación identidad

$$\begin{array}{rccc} \mathrm{id}: & G & \longrightarrow & G \\ & g & \mapsto & g \end{array}$$

es un homomorfismo de grupos.

(2) Sean G, G' grupos. La aplicación

$$\begin{array}{ccc} G & \longrightarrow & G' \\ g & \mapsto & 1_{G'} \end{array}$$

es un homomorfismo de grupos.

(3) Sea G grupo y sea H subgrupo de G. La inclusión

$$\begin{array}{rccc} i: & H & \longrightarrow & G \\ & h & \mapsto & h \end{array}$$

es un homomorfismo de grupos.

Ejemplo 6.1.4. Sean $(R,+,\cdot)$, $(S,+,\cdot)$ dos anillos y sea φ un homomorfismo de anillos entre R y S. Entonces φ es un homomorfismo de grupos entre $(R,+)$ y $(S,+)$.

Observación 6.1.5. Muchos de los conceptos que vamos a ver sobre homomorfismos en esta sección resultarán muy familiares. Esto se debe a que, como nos dice el ejemplo 6.1.4, los homomorfismos de anillos son también homomorfismos de grupos. Por ello las nociones, resultados y demostraciones siguientes repiten lo visto para homomorfismos de anillos en lo que respecta a la operación $+$. Puedes hacer el ejercicio de, en los argumentos para homomorfismos de anillos, sustituir la notación aditiva por notación multiplicativa. Aunque el grupo aditivo de un anillo es un grupo abeliano y los grupos que consideramos ahora pueden ser abelianos o no, esto no influye en los argumentos, por lo que, después del cambio de notación, obtendrás las definiciones, enunciados y argumentos para homomorfismos de grupos a partir de las definiciones, enunciados y argumentos para homomorfismos de anillos.

Ejemplos 6.1.6. (1) Sean $(R,+,\cdot)$, $(S,+,\cdot)$ dos anillos unitarios y sea φ un homomorfismo de anillos unitarios entre R y S. Entonces $\varphi|_{U(R)}$ es un homomorfismo de grupos entre $(U(R),\cdot)$ y $(U(S),\cdot)$, ya que $\varphi(U(R)) \subset U(S)$.

(2) Sean $(V,+,\cdot\mathbf{k})$, $(W,+,\cdot\mathbf{k})$ dos espacios vectoriales sobre $\mathbf{k}$ y sea φ una aplicación lineal entre V y W. Entonces φ es un homomorfismo de grupos entre $(V,+)$ y $(W,+)$.

Ejemplos 6.1.7. (1) La aplicación

$$\begin{array}{rccc} \varphi: & (GL(n,\mathbf{k}),\cdot) & \longrightarrow & (\mathbf{k}^*,\cdot) \\ & M & \mapsto & \det M \end{array}$$

es un homomorfismo de grupos.

(2) La aplicación

$$\begin{array}{rccc} \varphi: & (O(n),\cdot) & \longrightarrow & (\mathbf{R}^*,\cdot) \\ & M & \mapsto & \det M \end{array}$$

es un homomorfismo de grupos.

(3) La aplicación

$$\begin{array}{rccc} \varphi: & (\mathbf{R},+) & \longrightarrow & (\mathbf{R}^*,\cdot) \\ & x & \mapsto & e^x \end{array}$$

es un homomorfismo de grupos.

(4) Recuerda que si $\alpha \in \mathbf{R}$, entonces $e^{\alpha i} = \cos\alpha + i\,\mathrm{sen}\alpha$. La aplicación

$$\begin{array}{rccc} \varphi: & (\mathbf{R},+) & \longrightarrow & (\mathbf{C}^*,\cdot) \\ & \theta & \mapsto & e^{2\pi\theta i} \end{array}$$

es un homomorfismo de grupos.

(5) Sean $x, y \in \mathbf{R}$. Recuerda que $e^{x+iy} = e^x \cdot e^{yi}$. La aplicación

$$\begin{array}{rccc} \varphi: & (\mathbf{C},+) & \longrightarrow & (\mathbf{C}^*,\cdot) \\ & z & \mapsto & e^{2\pi z i} \end{array}$$

es un homomorfismo de grupos.

Proposición 6.1.8. *Si $\varphi : G \longrightarrow G'$ y $\psi : G' \longrightarrow G''$ son homomorfismos de grupos, entonces la composición $\psi \circ \varphi : G \longrightarrow G''$ es un homomorfismo de grupos.*

Demostración. Sean $g_1, g_2 \in G$. Entonces

$$(\psi \circ \varphi)(g_1 g_2) = \psi(\varphi(g_1 g_2)) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1))\psi(\varphi(g_2)) = (\psi \circ \varphi)(g_1) \cdot (\psi \circ \varphi)(g_2).$$

□

Proposición 6.1.9. *Sean G, G' dos grupos, sea H un subgrupo de G y H' un subgrupo de G'. Sea $\varphi : G \longrightarrow G'$ un homomorfismo de grupos.*

(1) La imagen de H por φ, que es $\varphi(H) = \{\varphi(h) \mid h \in H\}$, es un subgrupo de G'.

(2) la imagen inversa de H' por φ, que es $\varphi^{-1}(H') = \{g \in G \mid \varphi(g) \in H'\}$, es un subgrupo de G.

Demostración. Sean $g_1', g_2' \in \varphi(H)$. Veamos que $g_1' g_2'^{-1} \in \varphi(H)$. Existen $h_1, h_2 \in H$ tales que $\varphi(h_1) = g_1'$ y $\varphi(h_2) = g_2'$. Entonces $\varphi(h_1 h_2'^{-1}) = \varphi(h_1)\varphi(h_2')^{-1} = g_1' g_2'^{-1}$ por lo que $g_1 g_2'^{-1} \in \varphi(H)$. Esto demuestra (1).
Sean $g_1, g_2 \in \varphi^{-1}(H')$. Veamos que $g_1 g_2^{-1} \in \varphi^{-1}(H')$. Como $g_1, g_2 \in \varphi^{-1}(H')$ tenemos que $\varphi(g_1), \varphi(g_2) \in H'$. Como H' es un subgrupo y φ es un homomorfismo de grupos, $\varphi(g_1 \cdot g_2^{-1}) = \varphi(g_1)(\varphi(g_2))^{-1} \in H'$. Entonces $g_1 g_2^{-1} \in \varphi^{-1}(H')$. Esto demuestra (2). □

Definición 6.1.10. Sea $\varphi : G \longrightarrow G'$ un homomorfismo de grupos. El *núcleo* de φ es

$$\mathrm{Ker}\varphi = \{g \in G \mid \varphi(g) = 1_{G'}\}.$$

Observación 6.1.11. Si φ es un homomorfismo de anillos entre dos anillos $(R,+,\cdot)$ y $(S,+,\cdot)$, entonces el núcleo que definimos para φ como homomorfismo de anillos es lo mismo que el núcleo para φ como homomorfismo de grupos entre $(R,+)$ y $(S,+)$.

Corolario 6.1.12. *Sea $\varphi : G \longrightarrow G'$ un homomorfismo de grupos. Entonces el núcleo de φ es un subgrupo de G y la imagen de φ es un subgrupo de G'.*

Demostración. El resultado se sigue de la proposición 6.1.9, ya que el núcleo de φ es $\varphi^{-1}(<1_{G'}>)$ y la imagen de φ es $\varphi(G)$. □

Proposición 6.1.13. *Un homomorfismo de grupos $\varphi : G \longrightarrow G'$ es inyectivo si y solo si el núcleo de φ es $<1_G>$.*

Demostración. Para cualquier homomorfismo de grupos φ, como el núcleo de φ es un subgrupo de G, tenemos que $<1_G>$ está contenido en el núcleo de φ. Supongamos ahora que φ es inyectivo. Queremos ver que el núcleo de φ está contenido en $<1_G>$, es decir, que si $g \in \text{Ker}\varphi$, entonces $g = 1_G$. Si $g \in \text{Ker}\varphi$, entonces $\varphi(g) = 1_{G'}$. Por la observación 6.1.2, $\varphi(1_G) = 1_{G'}$. Como φ es inyectiva y g y 1_G tienen la misma imagen por φ, concluimos que $g = 1_G$. Supongamos ahora que $\text{Ker}\varphi = <1_G>$. Sean $g_1, g_2 \in G$ tales que $\varphi(g_1) = \varphi(g_2)$. Entonces $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = 1_{G'}$, por lo que $g_1 g_2^{-1}$ pertenece al núcleo de φ, de donde $g_1 g_2^{-1} = 1_G$ y $g_1 = g_2$. □

Definición 6.1.14. Sean G y G' grupos y sea $\varphi : G \longrightarrow G'$ un homomorfismo de grupos.

(1) Decimos que φ es un *isomorfismo* de grupos si φ es una aplicación biyectiva.

(2) Decimos que G y G' son grupos *isomorfos* y escribimos $G \simeq G'$ si existe un isomorfismo de G a G'.

Proposición 6.1.15. *(1) Si $\varphi : G \longrightarrow G'$ y $\psi : G' \longrightarrow G''$ son isomorfismos de grupos, entonces la composición $\psi \circ \varphi : G \longrightarrow G''$ es un isomorfismo de grupos.*

(2) Si $\varphi : G \longrightarrow G'$ es un isomorfismo de grupos, entonces $\varphi^{-1} : G' \longrightarrow G$ es un isomorfismo de grupos.

Demostración. Si $\varphi : G \longrightarrow G'$ y $\psi : G' \longrightarrow G''$ son isomorfismos de grupos su composición es un homomorfismo de grupos por la proposición 6.1.8 y es una aplicación biyectiva pues la composición de aplicaciones biyectivas es biyectiva. Esto demuestra (1). Sea ahora $\varphi : G \longrightarrow G'$ un isomorfismo de grupos y sea φ^{-1} la aplicación inversa de φ, que es biyectiva. Por tanto solo nos queda ver que φ^{-1} es un homomorfismo de grupos. Sean $g_1', g_2' \in G'$. Veamos que $\varphi^{-1}(g_1' g_2') = \varphi^{-1}(g_1')\varphi^{-1}(g_2')$. Sea $g_1 = \varphi^{-1}(g_1')$ y $g_2 = \varphi^{-1}(g_2')$. En ese caso $\varphi(g_1) = g_1'$ y $\varphi(g_2) = g_2'$. Entonces $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = g_1' g_2'$, por lo que $\varphi^{-1}(g_1' g_2') = g_1 g_2 = \varphi^{-1}(g_1')\varphi^{-1}(g_2')$ como queríamos demostrar. Esto prueba (2). □

De la proposición 6.1.15 se sigue de forma inmediata el siguiente corolario:

Corolario 6.1.16. *El conjunto $Aut(G)$ de automorfismos de un grupo G (es decir, el conjunto de isomorfismos de grupos de G en G) es un subgrupo de $(Biy(G), \circ)$.*

Ejemplos 6.1.17. (1) El homomorfismo identidad del ejemplo 6.1.3 (1) es un isomorfismo de grupos.

(2) El núcleo del homomorfismo de grupos del ejemplo 6.1.3 (2) es G y la imagen es $<1_{G'}>$.

(3) El homomorfismo i del ejemplo 6.1.3 (3) es un homomorfismo inyectivo de grupos.

(4) Sean $(R,+,\cdot)$, $(S,+,\cdot)$ dos anillos y sea φ un isomorfismo de anillos entre R y S. Entonces φ es un isomorfismo de grupos entre $(R,+)$ y $(S,+)$.

(5) Sean $(R,+,\cdot)$, $(S,+,\cdot)$ dos anillos unitarios y sea φ un isomorfismo de anillos unitarios entre R y S. Entonces $\varphi|_{U(R)}$ es un isomorfismo de grupos entre $(U(R),\cdot)$ y $(U(S),\cdot)$, ya que $\varphi(U(R)) \subset U(S)$ y $\varphi^{-1}(U(S)) \subset U(R)$, de donde $\varphi(U(R)) = U(S)$.

(6) Sean $(V,+,\cdot\mathbf{k})$, $(W,+,\cdot\mathbf{k})$ dos espacios vectoriales sobre $\mathbf{k}$ y sea φ un isomorfismo de espacios vectoriales entre V y W. Entonces φ es un isomorfismo de grupos entre $(V,+)$ y $(W,+)$.

(7) El homomorfismo de grupos φ del ejemplo 6.1.7 (1) es sobreyectivo y su núcleo es $SL(n,\mathbf{k})$.

(8) La imagen del homomorfismo de grupos φ del ejemplo 6.1.7 (2) es $<-1>=\{1,-1\}$ y su núcleo es $SO(n)$.

(9) La imagen del homomorfismo de grupos φ del ejemplo 6.1.7 (3) es el subgrupo de $(\mathbf{R}^*,\cdot)$ formado por los números reales positivos. El núcleo de φ es $<0>$, por lo que φ es inyectiva.

(10) La imagen del homomorfismo de grupos φ del ejemplo 6.1.7 (4) es el subgrupo S^1 de $\mathbf{C}^*$ descrito en el ejemplo 5.2.5 (6) y su núcleo es $(\mathbf{Z},+)$.

(11) El homomorfismo de grupos φ del ejemplo 6.1.7 (5) es sobreyectivo y su núcleo es $(\mathbf{Z},+)$.

Ejemplo 6.1.18. Sea (A,V) un espacio afín sobre un cuerpo $\mathbf{k}$. Dado $v \in V$ sea

$$\begin{array}{rccc} t_v: & A & \longrightarrow & A \\ & p & \mapsto & p+v \end{array}$$

la *traslación* de vector v. La aplicación

$$\begin{array}{ccc} (V,+) & \longrightarrow & (\mathrm{Af}(A),\circ) \\ v & \mapsto & t_v \end{array}$$

es un homomorfismo de grupos inyectivo. Su imagen es $\mathrm{Tras}(A)$, el subgrupo de $\mathrm{Af}(A)$ formado por las traslaciones de A.

Para los siguientes ejemplos necesitamos recordar estos resultados de Álgebra Lineal:

Notación 6.1.19. (1) Sean V_1 y V_2 dos espacios vectoriales sobre un cuerpo $\mathbf{k}$, sea B_1 una base de V_1, sea B_2 una base de V_2 y sea $f : V_1 \longrightarrow V_2$ una aplicación lineal. Denotamos por $M_{B_1}^{B_2} f$ la matriz asociada a f respecto de las bases B_1 y B_2.

(2) Si $V = V_1 = V_2$ y $B = B_1 = B_2$ escribimos $M_B f$ en lugar de $M_B^B f$.

Teorema 6.1.20. *Sea V un espacio vectorial de dimensión n sobre un cuerpo $\mathbf{k}$. y sea B una base de V.*

(1) Sean f_1, f_2 dos endomorfismos de V (es decir, aplicaciones lineales de V en V). Entonces $M_B(f_1 \circ f_2) = M_B(f_1) \cdot M_B(f_2)$.

(2) Sea M una matriz $m \times m$ con elementos en $\mathbf{k}$. Existe un único endomorfismo f de V tal que $M_B(f) = M$.

(3) Un endomorfismo f de V es un automorfismo de V (es decir, es isomorfismo de espacios vectoriales) si y solo si $M_B(f)$ es una matriz invertible.

Teorema 6.1.21. *Sea V un espacio vectorial euclídeo de dimensión n y sea B una base ortonormal de V. Un endomorfismo f de V es una aplicación ortogonal de V si y solo si $M_B(f)$ es una matriz ortogonal.*

Ejemplo 6.1.22. Sea V un espacio vectorial de dimensión n sobre un cuerpo $\mathbf{k}$. Fijamos una base B de V. La aplicación

$$\begin{array}{rccc} \varphi : & (GL(V), \circ) & \longrightarrow & (GL(n, \mathbf{k}), \cdot) \\ & f & \mapsto & M_B(f) \end{array}$$

es un isomorfismo de grupos. En efecto, la aplicación φ acaba en $GL(n, \mathbf{k})$ por el teorema 6.1.20 (3) y es un homomorfismo de grupos por el teorema 6.1.20 (1). Por último φ es una aplicación biyectiva por el teorema 6.1.20 (2).

Ejemplo 6.1.23. Sea V un espacio vectorial euclídeo de dimensión n. Fijamos una base ortonormal B de V. La aplicación

$$\begin{array}{rccc} \varphi : & (O(V), \circ) & \longrightarrow & (O(n), \cdot) \\ & f & \mapsto & M_B(f) \end{array}$$

es un isomorfismo de grupos. En efecto, la aplicación φ acaba en $O(n)$ por el teorema 6.1.21 y es un homomorfismo de grupos por el teorema 6.1.20 (1). Por último φ es una aplicación biyectiva por los teoremas 6.1.20 (2) y 6.1.21.

Observación 6.1.24. Los ejemplos 6.1.22 y 6.1.23 nos dicen que $(GL(V), \circ)$ y $(GL(n, \mathbf{k}), \cdot)$ son grupos isomorfos y que $(O(V), \circ)$ y $(O(n), \cdot)$ son grupos isomorfos. Sin embargo, no son isomorfos de manera *canónica*, ya que los isomorfismos entre dichos grupos varían con la elección de la base en V.

6.2 Subgrupos normales

El propósito de esta sección es, dados un grupo G y un subgrupo suyo H, definir, en los casos en que sea posible, una estructura de grupo en el conjunto cociente G/R^H y/o en el conjunto cociente G/R_H, compatible con la estructura de grupo de G. Para ello lo primero que necesitamos es ver si es posible definir una operación interna en G/R^H o en G/R_H, compatible con la operación interna de G. Consideremos el caso G/R^H (el caso G/R_H es análogo). Para que la operación en G/R^H sea compatible con la operación en G deberíamos definirla usando representantes de las clases de equivalencia, es decir, si g_1H y g_2H son dos elementos de G/R^H, querríamos definir el producto de g_1H y g_2H como $(g_1g_2)H$. La cuestión ahora es ver si esa operación está bien definida, es decir, si para todo $g_1', g_2' \in G$ tales que $g_1H = g_1'H$ y $g_2H = g_2'H$ se tiene $(g_1g_2)H = (g_1'g_2')H$. Esta última igualdad equivale a que $g_1g_2R^Hg_1'g_2'$, es decir, a que $(g_1g_2)^{-1}(g_1'g_2') \in H$. Como $(g_1g_2)^{-1}(g_1'g_2') = g_2^{-1}(g_1^{-1}g_1')g_2'$, a pesar de que $g_1^{-1}g_1' \in H$ (porque eso equivale a que $g_1R^Hg_1'$ y esto a que $g_1H = g_1'H$), no tiene por qué ocurrir que $g_2^{-1}(g_1^{-1}g_1')g_2'$ pertenezca a H. Sí ocurriría si G fuera abeliano o, más en general, si $g_1^{-1}g_1'$ y g_2' conmutaran o g_2^{-1} y $g_1^{-1}g_1'$ conmutaran, ya que en ese caso $g_2^{-1}(g_1^{-1}g_1')g_2' = (g_2^{-1}g_2')(g_1^{-1}g_1') \in H$ o $g_2^{-1}(g_1^{-1}g_1')g_2' = (g_1^{-1}g_1')(g_2^{-1}g_2') \in H$, pues $g_2^{-1}g_2'$ también está en H al ser $g_2H = g_2'H$. Sin embargo ni G tiene por qué ser abeliano ni g_2^{-1} y $g_1^{-1}g_1'$ tienen por qué conmutar ni $g_1^{-1}g_1'$ y g_2' tienen por qué conmutar. Entonces, nuestro objetivo va a ser identificar la condición que ha de cumplir H para que, aun en esa situación, podamos definir en G/R^H una operación interna compatible con la operación interna de G. Esto es lo mismo que conseguir que la operación $(g_1H)(g_2H) = (g_1g_2)H$ esté bien definida. Para eso bastará con que exista un elemento $h' \in H$ tal que $(g_1^{-1}g_1')g_2' = g_2'h'$, ya que, en ese caso, $g_2^{-1}(g_1^{-1}g_1')g_2' = (g_2^{-1}g_2')h' \in H$. Como esto debe ocurrir para todo $g_1, g_2, g_1', g_2' \in G$, necesitaremos la condición anterior para todo $g \in G$ y para todo $h \in H$, es decir, necesitaremos que, para todo $g \in G$ y para todo $h \in H$ exista $h' \in H$ tal que $hg = gh'$. A los subgrupos de G que cumplan esta condición les llamaremos *subgrupos normales*. Antes de dar la definición de subgrupo normal, reescribimos la condición $hg = gh'$ en varias reformulaciones equivalentes. Para ello vemos primero la definición de *subgrupo conjugado*:

Proposición–Definición 6.2.1. *Sea G un grupo, sea H un subgrupo de G y sea $g \in G$. El conjunto $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ es un subgrupo de G isomorfo a H. Decimos que gHg^{-1} es un subgrupo conjugado de G.*

Demostración. Sean $h_1, h_2 \in H$ y $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$. Entonces

$$(gh_1g^{-1})(gh_2g^{-1})^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = g(h_1h_2^{-1})g^{-1} \in gHg^{-1},$$

por lo que gHg^{-1} es un subgrupo de G. Para ver que son H y gHg^{-1} son subgrupos isomorfos consideramos la aplicación

$$\begin{array}{rccc} \Psi_g: & H & \longrightarrow & gHg^{-1} \\ & h & \mapsto & ghg^{-1}. \end{array}$$

La aplicación Ψ_g es un homomorfismo de grupos, ya que, si $h_1, h_2 \in H$, entonces

$$\Psi_g(h_1h_2) = g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = \Psi_g(h_1)\Psi_g(h_2).$$

El homomorfismo Ψ_g es inyectivo ya que si $\Psi_g(h) = 1$, entonces $1 = ghg^{-1}$, de donde $1 = g^{-1}g = g^{-1}(ghg^{-1})g = h$, por lo que $\mathrm{Ker}\Psi_g =< 1 >$. El homomorfismo Ψ_g es sobreyectivo ya que si $g' \in gHg^{-1}$, entonces existe $h \in H$ tal que $g' = ghg^{-1}$, en cuyo caso $g' = \Psi_g(h)$. □

Proposición 6.2.2. *Sea G un grupo y sea H un subgrupo de G. Las siguientes afirmaciones son equivalentes:*

(i) Para todo $g \in G$ y todo $h \in H$ existe $h' \in H$ tal que $hg = gh'$.

(i') Para todo $g \in G$ y todo $h \in H$ existe $h' \in H$ tal que $gh = h'g$.

(ii) Para todo $g \in G$ y todo $h \in H$ existe $h' \in H$ tal que $g^{-1}hg = h'$.

(ii') Para todo $g \in G$ y todo $h \in H$ existe $h' \in H$ tal que $ghg^{-1} = h'$.

(iii) Para todo $g \in G$, $g^{-1}Hg \subset H$.

(iii') Para todo $g \in G$, $gHg^{-1} \subset H$.

(iv) Para todo $g \in G$, $H \subset g^{-1}Hg$.

(iv') Para todo $g \in G$, $H \subset gHg^{-1}$.

(v) Para todo $g \in G$, $g^{-1}Hg = H$.

(v') Para todo $g \in G$, $gHg^{-1} = H$.

(vi) Para todo $g \in G$, $Hg = gH$.

Demostración. Las afirmaciones con prima se obtienen de las afirmaciones sin prima escritas para g^{-1} y las afirmaciones sin prima se obtienen de las afirmaciones con prima escritas para g^{-1}, por lo que cada afirmación sin prima es equivalente a su correspondiente afirmación con prima.

Las afirmaciones (i) y (ii) son equivalentes de manera obvia. También son equivalentes de manera obvia las afirmaciones (ii) y (iii).

Si $g^{-1}Hg \subset H$, entonces $H = g(g^{-1}Hg)g^{-1} \subset gHg^{-1}$, por lo que (iii) implica (iv'). Por lo dicho más arriba (iv') implica (iv), por lo que (iii) implica (iv). Si $H \subset g^{-1}Hg$, entonces $gHg^{-1} \subset g(g^{-1}Hg)g^{-1} = H$, por lo que (iv) implica (iii'). Por lo dicho más arriba (iii') implica (iii), por lo que (iv) implica (iii).

Como (v) es equivalente a (iii) y (iv) y (iii) y (iv) son equivalentes, (v) es equivalente tanto a (iii) como a (iv). □

Finalmente si $g^{-1}Hg = H$, entonces $gH = g(g^{-1}Hg) = Hg$, por lo que (v) implica (vi). Por otro lado, si $Hg = gH$, entonces $g^{-1}Hg = g^{-1}(gH) = H$, por lo que (vi) implica (v).

Definición 6.2.3. Sea G un grupo y sea H un subgrupo de G. Decimos que H es un *subgrupo normal* de G y escribimos $H \lhd G$ si se cumple cualquiera de las condiciones (y, por tanto, todas) de la proposición 6.2.2.

Observación 6.2.4. De la condición (v') de la proposición 6.2.2 se deduce que un subgrupo H de un grupo G es un subgrupo normal de G si y solo si el único subgrupo conjugado de H es H.

Proposición 6.2.5. *Sea $\varphi : G \longrightarrow G'$ un homomorfismo de grupos. El núcleo de φ es un subgrupo normal de G.*

Demostración. Ya vimos que $\mathrm{Ker}\varphi$ es un subgrupo de G. Para ver que es un subgrupo normal comprobamos que se cumple la condición (iii') de la proposición 6.2.2. Sea $g \in G$. Un elemento de $g\,\mathrm{Ker}\varphi\, g^{-1}$ es de la forma ghg^{-1} para algún $h \in \mathrm{Ker}\varphi$. Entonces

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)(\varphi(g))^{-1} = \varphi(g)(\varphi(g))^{-1} = \varphi(g)(\varphi(g))^{-1} = 1_{G'}$$

por lo que todo elemento de $g\,\mathrm{Ker}\varphi\, g^{-1}$ está contenido en $\mathrm{Ker}\varphi$. □

Proposición 6.2.6. *Sea G un grupo y sea H un subgrupo de G. Las siguientes afirmaciones son equivalentes:*

(i) El subgrupo H es un subgrupo normal de G.

(ii) R_H y R^H son la misma relación de equivalencia.

(iii) $G/R_H = G/R^H$.

Demostración. Una relación de equivalencia está determinada por sus clases de equivalencia ya que, dado un elemento g, los elementos que están relacionados con g son los elementos que están en la clase de equivalencia de g. El apartado (vi) de la proposición 6.2.2 nos dice que H es normal si y solo si, para todo $g \in G$, la clase de g respecto de R_H y la clase de g respecto R^H coinciden, es decir, si y solo si las clases de equivalencia de R_H y de R^H son las mismas, es decir, si y solo si R_H y R^H son la misma relación de equivalencia. Esto demuestra que (i) es equivalente a (ii).

Las relaciones R_H y R^H son la misma relación de equivalencia si y solo si las clases de equivalencia de R_H y de R^H son las mismas. Como las clases de equivalencia de R^H son los elementos de G/R^H y las clases de equivalencia de R_H son los elementos de G/R_H, R^H y R^H son la misma relación de equivalencia si y solo si sus conjuntos cocientes G/R^H y G/R_H son iguales. □

Corolario 6.2.7. *Sea G un grupo. Si H es un subgrupo de G con índice $[G : H] = 2$, entonces H es un subgrupo normal de G.*

Demostración. Para ver que H es normal usaremos la proposición 6.2.6. Sea $g \notin H$. En ese caso g no está relacionado con 1 ni con la relación R^H ni con la relación R_H. Entonces $gH \neq 1H = H$ y $Hg \neq H1 = H$. Como G/R^H y G/R_H tienen cada uno dos elementos, $G/R^H = \{H, gH\}$ y $G/R_H = \{H, Hg\}$. Recordemos que las clases de equivalencia de una relación de equivalencia de G nos dan una partición de G, por lo que $G = H \sqcup gH = H \sqcup Hg$. Entonces $gH = Hg$ por lo que $G/R^H = G/R_H$. □

Definición 6.2.8. Sea G un grupo y sea H un subgrupo normal de G. Denotaremos como G/H al conjunto cociente $G/R_H = G/R^H$.

Ejemplos 6.2.9. (1) Cualquier subgrupo de un grupo abeliano es normal.

(2) De la proposición 6.2.5 y del ejemplo 6.1.17 (7) se sigue que $SL(n, \mathbf{k})$ es un subgrupo normal de $GL(n, \mathbf{k})$.

(3) El grupo $SO(n)$ es un subgrupo normal de $O(n)$. Esto se puede deducir a partir de la proposición 6.2.5 y del ejemplo 6.1.17 (8) o también usando el corolario 6.2.7 y el ejemplo 5.5.8 (3).

Para los siguientes ejemplos necesitamos recordar estos resultados de Geometría afín:

Proposición 6.2.10. *Sean $(A_1, V_1), (A_2, V_2), (A_3, V_3)$ tres espacios afines sobre un cuerpo $\mathbf{k}$ y sean $f : A_1 \longrightarrow A_2$ y $g : A_2 \longrightarrow A_3$ dos aplicaciones afines. Entonces la aplicación lineal asociada a $f_2 \circ f_1$ es $\vec{f_2} \circ \vec{f_1}$, donde $\vec{f_1}, \vec{f_2}$ son, respectivamente, las aplicaciones lineales asociadas a f_1 y f_2 .*

Proposición 6.2.11. *Sea (A, V) un espacio afín sobre un cuerpo $\mathbf{k}$ y sea $f : A \longrightarrow A$ una aplicación afín. Entonces f es un isomorfismo afín si y solo si $\vec{f}$ es un automorfismo de V.*

Teorema 6.2.12. *Sea (A, V) un espacio afín sobre un cuerpo $\mathbf{k}$, sea $\tilde{f}$ un endomorfismo de V y sean $o, o' \in A$. Existe una única aplicación afín $f : A \longrightarrow A$ tal que*

(i) $\vec{f} = \tilde{f}$; *y*

(ii) $f(o) = o'$.

Proposición 6.2.13. *Sea (A, V) un espacio afín sobre un cuerpo $\mathbf{k}$ y sea $f : A \longrightarrow A$ una aplicación afín. La aplicación f es una traslación si y solo si $\vec{f} = id_V$.*

Ejemplo 6.2.14. Sea (A, V) un espacio afín sobre un cuerpo $\mathbf{k}$. La aplicación

$$\begin{array}{rccc} \varphi : & \mathrm{Af}(A) & \longrightarrow & GL(V) \\ & f & \mapsto & \vec{f} \end{array}$$

es un homomorfismo de grupos sobreyectivo y su núcleo es Tras(A). Por tanto, por la proposición 6.2.5, Tras(A) es un subgrupo normal de Af(A). Así pues, por el ejemplo 6.1.18, (Af(A), $\circ$) tiene un subgrupo normal isomorfo a $(V, +)$.

Comprobamos todas las afirmaciones relativas a φ. Que la aplicación φ termina en $GL(V)$ se sigue la proposición 6.2.11. Que φ es un homomorfismo de grupos se sigue de la proposición 6.2.10. Que φ es sobreyectiva se sigue del teorema 6.2.12. Que el núcleo de φ es Tras(A) se sigue de la proposición 6.2.13.

6.3 Grupo cociente

Teorema 6.3.1. *Sea G un grupo y sea H un subgrupo normal de G.*

(1) La operación

$$\begin{array}{ccc} G/H \times G/H & \longrightarrow & G/H \\ (g_1H, g_2H) & \mapsto & (g_1g_2)H \end{array}$$

es una operación interna en G/H y está bien definida.

(2) El conjunto G/H junto con la operación interna del apartado (1) es un grupo. Si G es abeliano, entonces G/H también es abeliano.

(3) La aplicación

$$\begin{array}{rccc} \pi: & G & \longrightarrow & G/H \\ & g & \mapsto & gH, \end{array}$$

que llamaremos proyección canónica*, es un homomorfismo de grupos sobreyectivo y su núcleo es H.*

Demostración. Para probar el apartado (1), necesitamos ver que la operación descrita está bien definida. Para ello sean $g_1, g_2, g_1', g_2' \in G$ tales que $g_1H = g_1'H$ y $g_2H = g_2'G$ en G/H. Veamos que $(g_1g_2)H = (g_1'g_2')H$. Esto ocurrirá si y solo si $(g_1g_2)^{-1}(g_1'g_2') \in H$. Tenemos $(g_1g_2)^{-1}(g_1'g_2') = g_2^{-1}(g_1^{-1}g_1')g_2'$. Como $g_1H = g_1'H$, entonces $g_1^{-1}g_1' \in H$. Como $H \lhd G$, por la proposición 6.2.2 (i), existe $h' \in H$ tal que $(g_1^{-1}g_1')g_2' = g_2'h'$, de donde $(g_1g_2)^{-1}(g_1'g_2') = (g_2^{-1}g_2')h'$. Como $g_2H = g_2'H$, entonces $g_2^{-1}g_2' \in H$, por lo que $(g_2^{-1}g_2')h' \in H$ y $(g_1g_2)^{-1}(g_1'g_2') \in H$, de donde se sigue que $(g_1g_2)H = (g_1'g_2')H$ como queríamos.

La operación definida en (1) cumple las propiedades de la definición de grupo (definición 0.1.1) ya que la operación en G las cumple (podríamos decir que la operación definida en (1) "hereda" las propiedades de la operación en G al estar definida la primera a partir de la segunda usando representantes). En efecto, se cumple la propiedad asociativa, ya que dados $g_1, g_2, g_3 \in G$, como $g_1(g_2g_3) = (g_1g_2)g_3)$, se tiene

$$g_1H(g_2Hg_3H) = g_1H((g_2g_3)H) = (g_1(g_2g_3))H = ((g_1g_2)g_3))H = (g_1g_2)Hg_3H = (g_1Hg_2H)g_3H.$$

También existe un elemento neutro en G/H, que es la clase de 1_G, es decir, $1_G H = H$, ya que, como para todo $g \in G$, $g1_G = 1_G g = g$, se tiene

$$gH1_G H = (g1_G)H = gH = (1_G g)H = 1_G HgH.$$

Finalmente, todo elemento de G/H tiene inverso. En efecto, dado $g \in G$ y sea g^{-1} el inverso de g en G. Entonces $gg^{-1} = g^{-1}g = 1_G$, por lo que

$$gHg^{-1}H = (gg^{-1})H = 1_G H = (g^{-1}g)H = g^{-1}HgH,$$

así que el inverso de gH es la clase $g^{-1}H$ de g^{-1}. Además, si la operación en G es conmutativa, se ve de manera análoga que la operación definida en (1) también lo es.
Que la aplicación π es un homomorfismo de grupos se sigue de manera inmediata de la definición de la operación de G/H. Es sobreyectiva ya que, dada una clase $gH \in G/H$, $\pi(g) = gH$. El núcleo de π están formado por aquellos elementos $g \in G$ tales que $\pi(g) = gH$ es el neutro de G/H, es decir, aquellos elementos $g \in G$ relacionados con 1_G, es decir, aquellos elementos de G que pertenecen a H. □

Observación 6.3.2. La razón por la que hemos necesitado comprobar que la operación del apartado (1) del teorema 6.3.1 está bien definida, es por ser una operación en un conjunto cociente que se ha definido usando representantes.

Teorema 6.3.3. *(de isomorfía). Sea $\varphi : G \longrightarrow G'$ un homomorfismo de grupos, sea $H = Ker\varphi$ y sea $H' = im\varphi$.*

(1) La aplicación

$$\begin{array}{rccc} \overline{\varphi}: & G/H & \longrightarrow & H' \\ & gH & \mapsto & \varphi(g) \end{array}$$

está bien definida y es un isomorfismo de grupos.

(2) El homomorfismo φ se descompone como $\varphi = i \circ \overline{\varphi} \circ \pi$, donde π es la proyección canónica del apartado (3) del teorema 6.3.1 e i es la inclusión de H' en G'.

Demostración. Para demostrar que $\overline{\varphi}$ está bien definida, sean $g_1, g_2 \in G$ tales que $g_1 H = g_2 H$. Queremos ver que $\varphi(g_1) = \varphi(g_2)$. Si $g_1 H = g_2 H$, entonces $g_1^{-1} g_2 \in H = \text{Ker}\varphi$, por lo que $1_{G'} = \varphi(g_1^{-1} g_2) = \varphi(g_1)^{-1}\varphi(g_2)$, de donde $\varphi(g_1) = \varphi(g_2)$.
La aplicación $\overline{\varphi}$ es un homomorfismo de grupos ya que si $g_1 H, g_2 H \in G/H$, entonces

$$\overline{\varphi}(g_1 H g_2 H) = \overline{\varphi}((g_1 g_2)H) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1 H)\overline{\varphi}(g_2 H).$$

El homomorfismo $\overline{\varphi}$ es sobreyectivo ya que, si $g' \in H' = \text{im}\varphi$, entonces existe $g \in G$ tal que $\varphi(g) = g'$, por lo que $\overline{\varphi}(gH) = \varphi(g) = g'$.
El homomorfismo $\overline{\varphi}$ es inyectivo porque $\text{Ker}\overline{\varphi}$ es

$$\{gH \in G/H \mid \overline{\varphi}(gH) = 1_{G'}\} = \{gH \in G/H \mid \varphi(g) = 1_{G'}\} = \{gH \in G/H \mid g \in H\} = \{1_G H\},$$

es decir, el núcleo de $\overline{\varphi}$ es trivial.
La igualdad $\varphi = i \circ \overline{\varphi} \circ \pi$ se sigue de manera inmediata de la definición de $\overline{\varphi}$. □

Observación 6.3.4. De nuevo la demostración del teorema 6.3.3 es la misma que la demostración del teorema de isomorfía de anillos una vez que en aquella se cambia la notación aditiva por multiplicativa y se prescinde de la parte relativa a la operación producto de los anillos.

Para la demostración del corolario 6.3.6 necesitaremos el lema siguiente:

Lema 6.3.5. *Los subgrupos de* $(\mathbf{Z},+)$ *son los ideales de* $(\mathbf{Z},+,\cdot)$. *Si* $x \in \mathbf{Z}$, *entonces el subgrupo* $<x>$ *es el ideal* (x).

Demostración. Un ideal I de $(\mathbf{Z},+,\cdot)$ cumple que, para cada $x, y \in I$, $x - y \in I$. Por tanto, un ideal I de $(\mathbf{Z},+,\cdot)$ es un subgrupo de $(\mathbf{Z},+)$.
Un subgrupo H de $(\mathbf{Z},+)$ cumple, para cada $x, y \in I$, $x + y \in H$. Sea ahora $n \in \mathbf{Z}$ y $x \in H$. Si $n \in \mathbf{N}$, entonces $nx = x + \overset{n)}{\cdots} + x \in H$, por ser H subgrupo y pertenecer x a H. Si $n = 0$, entonces $0x = 0 \in H$, por ser H subgrupo. Finalmente, si $n \in \mathbf{Z}$ y $n < 0$, entonces $nx = (-x) + \overset{-n)}{\cdots} + (-x) \in H$, ya que, al ser H subgrupo y pertenecer x a H, tenemos que $-x \in H$. Por tanto, para todo $n \in \mathbf{Z}$ y $x \in H$, $nx \in H$, por lo que H es un ideal.
Los elementos del ideal generado por x son todos los números enteros de la forma nx, donde $n \in \mathbf{Z}$. Si $n > 0$, entonces $nx = x + \overset{n)}{\cdots} + x$ como ya se ha señalado. Si $n = 0$, entonces $0x = 0$. Finalmente, si $n < 0$, entonces $nx = (-x) + \overset{-n)}{\cdots} + (-x)$. Estos son justamente los elementos del subgrupo cíclico generado por x. □

Corolario 6.3.6. *Sea* $(G,\cdot)$ *un grupo cíclico. Entonces* G *es isomorfo a* $(\mathbf{Z},+)$ *o a* $(\mathbf{Z}_n,+)$. *Lo primero ocurre si y solo si* G *es infinito. Lo segundo ocurre si y solo si* G *es finito de orden* n.

Demostración. El resultado es un corolario del teorema 6.3.3. Sea $g \in G$ tal que $G = <g>$. Consideramos la aplicación

$$\begin{array}{rccc} \varphi: & (\mathbf{Z},+) & \longrightarrow & (G,\cdot) \\ & n & \mapsto & g^n. \end{array}$$

La aplicación φ es un homomorfismo de grupos por (5.1.2). Además, por la definición de $<g>$, φ es sobreyectivo. Pueden ocurrir dos cosas: que $\mathrm{Ker}\varphi = <0>$ o que $\mathrm{Ker}\varphi \neq <0>$. En el primer caso por el teorema 6.3.3, $(\mathbf{Z},+)$ y $(G,\cdot)$ son isomorfos y $(G,\cdot)$ es infinito. En el segundo caso $\mathrm{Ker}\varphi$ es un subgrupo no nulo, así que, por el lema 6.3.5 y por el ejemplo 3.2.3 (1), existe $n \in \mathbf{N}$ tal que $\mathrm{Ker}\varphi = <n>$. En ese caso por el teorema 6.3.3 $(\mathbf{Z}/<n>,+)$ y $(G,\cdot)$ son isomorfos. Por el lema 6.3.5, $<n> = (n)$; además, según la observación 5.5.3, la relación de equivalencia definida en $(\mathbf{Z},+)$ por el subgrupo $<n>$ es la misma que la relación de equivalencia definida en $(\mathbf{Z},+,\cdot)$ por el ideal (n), por lo que el grupo cociente $(\mathbf{Z}/<n>,+)$ es lo mismo que el grupo aditivo $(\mathbf{Z}/(n),+)$ del anillo $(\mathbf{Z}/(n),+,\cdot)$. Como los anillos $(\mathbf{Z}/(n),+,\cdot)$ y $(\mathbf{Z}_n,+,\cdot)$ son isomorfos, los grupos $(\mathbf{Z}/(n),+)$ y $(\mathbf{Z}_n,+)$ son grupos isomorfos según asegura el ejemplo 6.1.4, por lo que $(\mathbf{Z}_n,+)$ y $(G,\cdot)$ son grupos isomorfos. Como $\mathbf{Z}_n$ tiene n elementos, G es finito y su orden es n. □

Tema 7

El grupo simétrico

7.1 Primeras definiciones

Recordamos los ejemplos 5.1.5 (2) y 5.4.3 (1):

Proposición–Definición 7.1.1. El conjunto S_n de las aplicaciones biyectivas de $\{1, 2, \ldots, n\}$ en $\{1, 2, \ldots, n\}$ es un grupo con respecto a la composición de aplicaciones. El orden de S_n es $n!$. A S_n lo llamamos *grupo simétrico*.

Observación 7.1.2. La definición de S_n que acabamos de dar es en realidad un "modelo" concreto de S_n. De hecho, si A es un conjunto de n elementos, entonces $(\mathrm{Biy}(A), \circ)$ es isomorfo a S_n y podemos tomar $\mathrm{Biy}(A)$ como otro modelo de S_n. Para ver que $(\mathrm{Biy}(A), \circ)$ y S_n son isomorfos establecemos un isomorfismo entre ambos. Para ello elegimos una aplicación biyectiva φ entre A y $\{1, 2, \ldots, n\}$ (tal aplicación biyectiva siempre existe ya que A y $\{1, 2, \ldots, n\}$ son conjuntos finitos con el mismo número de elementos) y consideramos la aplicación

$$\begin{array}{rccc} \Phi: & \mathrm{Biy}(A) & \longrightarrow & S_n \\ & \tau & \mapsto & \varphi \circ \tau \circ \varphi^{-1}. \end{array}$$

La aplicación Φ es un isomorfismo de grupos. En efecto, si $\tau_1, \tau_2 \in \mathrm{Biy}(A)$, entonces

$$\Phi(\tau_1 \circ \tau_2) = \varphi \circ (\tau_1 \circ \tau_2) \circ \varphi^{-1} = (\varphi \circ \tau_2 \circ \varphi^{-1}) \circ (\varphi \circ \tau_1 \circ \varphi^{-1}) = \Phi(\tau_1) \circ \Phi(\tau_2),$$

por lo que Φ es un homomorfismo de grupos. Por otra parte Φ es biyectivo ya que tiene una aplicación inversa, que es

$$\begin{array}{rccc} \Psi: & S_n & \longrightarrow & \mathrm{Biy}(A) \\ & \sigma & \mapsto & \varphi^{-1} \circ \sigma \circ \varphi. \end{array}$$

Notación 7.1.3. (1) Sea $\sigma \in S_n$. Usaremos para σ la siguiente notación, que con un vistazo nos permite saber la imagen por σ de cada elemento de $\{1, 2, \ldots, n\}$:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Observamos que σ viene determinada por la segunda fila de la matriz anterior, que es una *permutación* de la n-upla $(1, 2, \ldots, n)$. Por eso a los elementos de S_n se les llama permutaciones y a S_n *grupo de permutaciones de n elementos*.

(2) Aunque la operación del grupo S_n es la composición, normalmente la llamaremos producto. Así, si $\sigma, \tau \in S_n$, usualmente escribiremos $\sigma \cdot \tau$ o $\sigma\tau$ en vez de $\sigma \circ \tau$.[1]

Ejemplo 7.1.4. Sea σ el elemento de S_5

$$\begin{array}{rccc} \sigma: & \{1,2,\ldots,n\} & \longrightarrow & \{1,2,\ldots,n\} \\ & 1 & \mapsto & 2 \\ & 2 & \mapsto & 5 \\ & 3 & \mapsto & 1 \\ & 4 & \mapsto & 4 \\ & 5 & \mapsto & 3 \end{array}$$

Según la notación 7.1.3,

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

Definición 7.1.5. Sea $k \in \mathbf{N}, k \leq n$, sea $\{i_1, i_2, \ldots, i_k\}$ un subconjunto de k elementos (distintos) de $\{1, 2, \ldots, n\}$ y sea $\sigma \in S_n$ tal que $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{k-1}) = \sigma(i_k), \sigma(i_k) = i_1$ y $\sigma(j) = j$ para todo $j \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$. En ese caso diremos que σ es un *ciclo de longitud k* o un *k−ciclo* y usaremos la notación

$$\sigma = \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_{k-1} & i_k \end{pmatrix}.$$

A los 2-ciclos los llamaremos *trasposiciones*.

Observación 7.1.6. (1) De acuerdo con la definición 7.1.5 podemos decir que la identidad es un 1-ciclo.

(2) El orden de un k-ciclo es k. En efecto, dado el k-ciclo $\sigma = \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_{k-1} & i_k \end{pmatrix}$, para todo $m \in \mathbf{N}$, $m < k$, tenemos $\sigma^m(i_1) = \sigma^{m-1}(i_2) = \cdots = \sigma(i_{m-1}) = i_m \neq i_1$, por lo que $\sigma^m \neq \mathrm{id}$. En cambio, para todo $i_j \in \{i_1, i_2, \ldots, i_k\}$, se tiene $\sigma^k(i_j) = \sigma^j(\sigma^{k-j}(i_j)) = \sigma^j(i_k) = \sigma^{j-1}(\sigma(i_k)) = \sigma^{j-1}(i_1) = i_j$, por lo que $\sigma^k = \mathrm{id}$.

[1] Como acabamos de decir, nosotros vamos a convenir que $\sigma\tau$ signifique $\sigma \circ \tau$. Esta convención no es universal y hay textos en los que se adopta la contraria, es decir, que $\sigma\tau$ signifique $\tau \circ \sigma$. Esto ocurre, por ejemplo, en *Estructuras Algebraicas: Teoría Elemental de Grupos*, de J.F. Fernando y J.M. Gamboa y en los apuntes de *Estructuras Algebraicas* de M. González. En cambio, hay otros libros, como por ejemplo *Álgebra lineal y geometría*, de M. Castellet e I. Llerena, que adoptan la misma convención que nosotros. Así pues, al consultar otros textos, debes tener cuidado de comprobar primero qué convención emplean. En cualquier caso, ambas convenciones son equivalentes en el sentido de que los grupos que se obtienen usando una y otra operación son isomorfos.

Definición 7.1.7. (1) Sea $\sigma \in S_n$. El *soporte* de σ es el conjunto

$$\mathrm{sop}(\sigma) = \{i \in \{1, 2, \ldots, n\} \mid \sigma(i) \neq i\}.$$

(2) Decimos que $\sigma, \tau \in S_n$ son permutaciones *disjuntas* si sus soportes son disjuntos.

Observación 7.1.8. Sea $k \in \mathbf{N}, k \geq 2$. El soporte del k-ciclo $(i_1 i_2 \ldots i_k)$ es $\{i_1, i_2, \ldots, i_k\}$.

Proposición 7.1.9. *El producto de dos permutaciones disjuntas de S_n es conmutativo.*

Demostración. Sean $\sigma, \tau \in S_n$ dos permutaciones disjuntas. Para ver que $\sigma \circ \tau = \tau \circ \sigma$ comprobamos que, para todo $i \in \{1, 2, \ldots, n\}$, se tiene $(\sigma \circ \tau)(i) = (\tau \circ \sigma)(i)$. Puesto que $\mathrm{sop}(\sigma) \cap \mathrm{sop}(\tau) = \emptyset$,

$$\{1, 2 \ldots, n\} = \mathrm{sop}(\sigma) \sqcup \mathrm{sop}(\tau) \sqcup (\mathrm{sop}(\sigma) \cup \mathrm{sop}(\tau))^c,$$

donde $\sqcup$ quiere decir unión disjunta y $(\mathrm{sop}(\sigma) \cup \mathrm{sop}(\tau))^c$ es el complementario de $\mathrm{sop}(\sigma) \cup \mathrm{sop}(\tau)$ en $\{1, 2 \ldots, n\}$. Evaluamos $\sigma \circ \tau$ y $\tau \circ \sigma$ en cada i de $\{1, 2 \ldots, n\}$.

Caso 1: $i \in \mathrm{sop}(\sigma)$. En ese caso $\sigma(i) \in \mathrm{sop}(\sigma)$, ya que no es posible que $\sigma^2(i) = \sigma(i)$ pues, si esto último ocurriera, aplicando σ^{-1} a $\sigma^2(i) = \sigma(i)$ obtendríamos $\sigma(i) = i$, por lo que i no pertenecería al soporte de σ, en contra de nuestra hipótesis. Entonces ni i ni $\sigma(i)$ pertenecen al soporte de τ y tenemos $(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i)$ y $(\tau \circ \sigma) = \tau(\sigma(i)) = \sigma(i)$.

Caso 2: $i \in \mathrm{sop}(\tau)$. Razonando de forma análoga al caso 1 se comprueba que $(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \tau(i)$ y $(\tau \circ \sigma) = \tau(\sigma(i)) = \tau(i)$.

Caso 3: $i \notin \mathrm{sop}(\sigma) \cup \mathrm{sop}(\tau)$. En este caso $(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i) = i$ y $(\tau \circ \sigma) = \tau(\sigma(i)) = \tau(i) = i$. □

Ejemplos 7.1.10. (1) La permutación σ del ejemplo 7.1.4 es un 4-ciclo. En efecto,

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

Comprobamos que σ tiene orden 4: $\sigma^2 = \begin{pmatrix} 1 & 5 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}$, $\sigma^3 = \begin{pmatrix} 1 & 3 & 5 & 2 \end{pmatrix}$ y $\sigma^4 = \mathrm{id}$.

(2) La permutación σ^2 del apartado anterior y la permutación

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 6 & 7 & 4 & 5 \end{pmatrix}$$

de S_7 no son ciclos. Sin embargo, según vimos en el apartado (1), σ^2 se puede escribir como producto de ciclos disjuntos. Por otra parte, $\tau = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 4 & 6 \end{pmatrix}\begin{pmatrix} 5 & 7 \end{pmatrix}$, por lo que τ también se puede escribir como producto de ciclos disjuntos.

7.2 Descomposición de una permutación

Acabamos de ver en el ejemplo 7.1.10 (2) dos permutaciones que podían ser escritas como producto de ciclos disjuntos. Demostramos a continuación que esto ocurre siempre.

Proposición 7.2.1. *Toda permutación σ de S_n se puede escribir como producto de ciclos disjuntos de S_n la unión de cuyos soportes es el soporte de σ.*

Demostración. Sea σ una permutación. Demostramos el resultado usando inducción completa sobre el cardinal del soporte de σ. Si el soporte de σ es vacío, entonces σ es la identidad, que, según la observación 7.1.6, es un 1-ciclo, por lo que el resultado es cierto. Sea ahora $m \in \mathbf{N}$ el cardinal del soporte de σ y supongamos que el enunciado es cierto para permutaciones cuyo soporte tiene cardinal menor que m. Entonces la permutación σ no es la identidad. En ese caso existe algún $i \in \{1, 2, \ldots, n\}$ tal que $\sigma(i) \neq i$. Como S_n es un grupo finito, σ tiene orden finito $l \in \mathbf{N}$ por lo que σ^l es la permutación identidad y en particular $\sigma^l(i) = i$. Sea k el mínimo número natural tal que $\sigma^k(i) = i$. Entonces los números $i, \sigma(i), \sigma^2(i), \ldots, \sigma^{k-1}(i)$ son elementos distintos de $\{1, 2, \ldots, n\}$, ya que, si $r, s \in \mathbf{N}$ y, por ejemplo, $0 \leq r \leq s < k$ y $\sigma^r(i) = \sigma^s(i)$, entonces $\sigma^{-r}(\sigma^r(i)) = \sigma^{-r}(\sigma^s(i))$, de donde $\sigma^{s-r}(i) = i$. Como $s - r \leq s < k$ y k es el mínimo número natural tal que $\sigma^k(i) = i$, se tiene que $s - r = 0$, es decir, $s = r$. En particular $i, \sigma(i), \sigma^2(i), \ldots, \sigma^{k-1}(i)$ pertenecen al soporte de σ. Sea σ_1 el ciclo $\begin{pmatrix} i & \sigma(i) & \sigma^2(i) & \cdots & \sigma^{k-2}(i) & \sigma^{k-1}(i) \end{pmatrix}$. Entonces la permutación $\sigma_1^{-1}\sigma$ deja $i, \sigma(i), \sigma^2(i), \ldots, \sigma^{k-2}(i), \sigma^{k-1}(i)$ fijos, por lo que el soporte de $\sigma_1^{-1}\sigma$ es $\mathrm{sop}(\sigma) \setminus \{i, \sigma(i), \sigma^2(i), \ldots, \sigma^{k-1}(i)\}$ y

$$\mathrm{sop}(\sigma) = \mathrm{sop}(\sigma_1) \sqcup \mathrm{sop}(\sigma_1^{-1}\sigma). \tag{7.2.1.1}$$

En particular el cardinal del soporte de $\sigma_1^{-1}\sigma$ es menor que m. Entonces, por la hipótesis de inducción, existen ciclos disjuntos $\sigma_2, \sigma_3, \ldots, \sigma_s$ tales que

$$\sigma_1^{-1}\sigma = \sigma_2\sigma_3 \cdots \sigma_s \tag{7.2.1.2}$$

y cuyos soportes cumplen

$$\mathrm{sop}(\sigma_1^{-1}\sigma) = \mathrm{sop}(\sigma_2) \sqcup \mathrm{sop}(\sigma_3) \sqcup \cdots \sqcup \mathrm{sop}(\sigma_s). \tag{7.2.1.3}$$

Multilpicando por σ_1 ambos lados de (7.2.1.2) obtenemos

$$\sigma = \sigma_1\sigma_2\sigma_3 \cdots \sigma_s$$

y de (7.2.1.1) y (7.2.1.3) obtenemos que el soporte de σ_1 es disjunto con el soporte de cada uno de los ciclos $\sigma_2, \sigma_3, \ldots, \sigma_s$ y

$$\mathrm{sop}(\sigma) = \mathrm{sop}(\sigma_1) \sqcup \mathrm{sop}(\sigma_2) \sqcup \mathrm{sop}(\sigma_3) \sqcup \cdots \sqcup \mathrm{sop}(\sigma_s).$$

□

Observación 7.2.2. En el tema 8 veremos que los ciclos (de lóngitud mayor que 1) disjuntos que aparecen en la descomposición de una permutación de S_n dada están determinados de forma única, es decir, una permutación se escribe de manera única como producto de ciclos disjuntos de lóngitud mayor que 1 salvo por el orden en el que escribimos los ciclos, ya que dos ciclos disjuntos conmutan.

Proposición 7.2.3. *Todo ciclo se escribe como producto de trasposiciones. Concretamente*

$$\sigma = \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_{k-1} & i_k \end{pmatrix} = \begin{pmatrix} i_1 & i_2 \end{pmatrix} \begin{pmatrix} i_2 & i_3 \end{pmatrix} \cdots \begin{pmatrix} i_{k-1} & i_k \end{pmatrix}.$$

Demostración. La demostración es una comprobación inmediata. □

Como consecuencia inmediata de las proposiciones 7.2.1 y 7.2.3 tenemos el siguiente corolario:

Corolario 7.2.4. *(1) El grupo S_n está generado por sus ciclos.*

(2) Toda permutación de S_n se escribe como producto de trasposiciones, en general no disjuntas. Por tanto el grupo S_n está generado por sus trasposiciones.

La demostración de la proposición 7.2.1 se puede reescribir como un algoritmo para hallar los ciclos que aparecen en la descomposición de una permutación dada. Explicamos este algoritmo en la primera parte del siguiente ejemplo:

Ejemplo 7.2.5. Consideramos la permutación

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

de S_{13}.

(i) *Descomposición de σ como producto de ciclos disjuntos.* En la primera fila buscamos la primera entrada i tal que $\sigma(i) \neq i$, es decir, la primera entrada i tal que la entrada en la segunda fila y la columna i-ésima es diferente de i. En nuestro caso $i = 2$. Vemos cuál es la entrada en la segunda fila y la segunda columna, que en nuestro caso es 5, miramos la segunda entrada de la quinta columna, que en nuestro caso el 8; miramos la entrada de la octava columna y vemos que es 2, que era nuestro valor de i. Entonces consignamos el ciclo $\begin{pmatrix} 2 & 5 & 8 \end{pmatrix}$. Ahora buscamos en la primera fila la primera entrada j tal que $\sigma(j) \neq j$ y j no pertenezca al soporte del ciclo que acabamos de consignar; en nuestro caso ese soporte es $\{2, 5, 8\}$ y $j = 3$. Repetimos para j el procedimiento que hemos llevado a cabo para i, obteniendo así el ciclo $\begin{pmatrix} 3 & 4 & 7 & 12 \end{pmatrix}$, que también consignamos. Buscamos ahora en la primera fila la primera entrada k tal que $\sigma(k) \neq k$ y k no pertenezca al soporte de los ciclos $\begin{pmatrix} 2 & 5 & 8 \end{pmatrix}$ y $\begin{pmatrix} 3 & 4 & 7 & 12 \end{pmatrix}$; en nuestro $k = 9$. Repitiendo para k el proceso que hemos llevado a cabo con i y j obtenemos el ciclo $\begin{pmatrix} 9 & 13 & 11 & 10 \end{pmatrix}$. En nuestro caso la unión de

los soportes de los tres ciclos obtenidos y del conjunto de elementos que σ deja fijos (que es $\{1,6\}$) es todo el conjunto $\{1,2,3,4,5,6,7,8,9,10,11,12,13\}$ por lo que nuestro algoritmo terminaría aquí y la descomposición de σ como producto de ciclos disjuntos sería

$$\sigma = \begin{pmatrix} 2 & 5 & 8 \end{pmatrix}\begin{pmatrix} 3 & 4 & 7 & 12 \end{pmatrix}\begin{pmatrix} 9 & 13 & 11 & 10 \end{pmatrix}. \tag{7.2.5.1}$$

(ii) *Descomposición de σ como producto de trasposiciones.* Aplicando a cada ciclo de (7.2.5.1) la proposición 7.2.3 obtenemos

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

La descomposición de una permutación como producto de ciclos disjuntos nos permite calcular su orden de manera sencilla. Si los ciclos de la descomposición tienen longitud $k_1, k_2, \ldots, k_s$, es intuitivamente claro que el orden de la permutación será el mínimo común múltiplo de $k_1, k_2, \ldots, k_s$. Para ello basta pensar gráficamente los ciclos como s ruedas, cada una de las cuales tiene marcados en su circunferencia los k_i números del soporte del ciclo correspondiente, en una ordenación adecuada y delimitando porciones de arco iguales. Cada segundo, cada rueda gira, en sentido horario por ejemplo, un ángulo $2\pi/k_i$, de manera que cada número de la circunferencia pasa a ocupar la posición que tenía en la rueda el número siguiente. Es claro que la primera vez que los números de todas las ruedas vuelven a estar en la posición de partida es cuando han transcurrido un número de segundos igual al mínimo común múltiplo de $k_1, k_2, \ldots, k_s$. Daremos de todas maneras una demostración formal de cuál es el orden de una permutación. Para ello necesitamos ver una proposición:

Proposición 7.2.6. *Sean σ y τ dos permutaciones disjuntas de S_n.*

(1) $< \sigma > \cap < \tau > = \{\mathrm{id}\}$.

(2) El orden de $\sigma\tau$ es el mínimo común múltiplo del orden de σ y el orden de τ.

Demostración. Un elemento ρ de $< \sigma > \cap < \tau >$ es de la forma $\rho = \sigma^s = \tau^t$. Si i queda fijo por σ, entonces i también queda fijo por σ^s y si j queda fijo por τ, entonces j también queda fijo por τ^t. Entonces $\mathrm{sop}(\sigma^s) \subset \mathrm{sop}(\sigma)$ y $\mathrm{sop}(\tau^t) \subset \mathrm{sop}(\tau)$, de donde $\mathrm{sop}(\rho) \subset \mathrm{sop}(\sigma) \cap \mathrm{sop}(\tau) = \emptyset$, por lo que $\rho = \mathrm{id}$. Esto demuestra (1).
Sea n_1 el orden de σ, sea n_2 el orden de τ y sea $m = \mathrm{m.c.m.}(n_1, n_2)$. Como σ y τ son permutaciones disjuntas, $\sigma\tau = \tau\sigma$ por la proposición 7.1.9, por lo que tenemos $(\sigma\tau)^m = \sigma^m\tau^m$. Como m es múltiplo de n_1 y n_2, por el corolario 5.4.8 tememos

$$(\sigma\tau)^m = \sigma^m\tau^m = \mathrm{id}. \tag{7.2.6.1}$$

Sea ahora $k \in \mathbf{N}$ tal que $(\sigma\tau)^k = \mathrm{id}$. Entonces $\mathrm{id} = (\sigma\tau)^k = \sigma^k\tau^k$, por lo que $\sigma^k = \tau^{-k}$ es un elemento de $< \sigma > \cap < \tau >$, que es $\{\mathrm{id}\}$. Por el corolario 5.4.8, n_1 divide a k y n_2 divide a $-k$ y, por tanto, a k. Entonces k es un múltiplo común de n_1 y n_2, por lo que $m \leq k$. Esto junto con (7.2.6.1) demuestra que m es el orden de $\sigma\tau$ (véase la proposición 5.4.6). □

Corolario 7.2.7. *Sea σ una permutación de S_n, sean $\sigma_1, \sigma_2, \ldots, \sigma_s$ ciclos disjuntos y sean $k_1, k_2, \ldots, k_s$ las longitudes respectivas de $\sigma_1, \sigma_2, \ldots, \sigma_s$. Si $\sigma = \sigma_1\sigma_2\cdots\sigma_s$, entonces el orden de σ es el mínimo común múltiplo de $k_1, k_2, \ldots, k_s$.*

Demostración. El corolario se demuestra por inducción a partir de la observación 7.1.6 (2) y de la proposición 7.2.6. □

Ejemplos 7.2.8. El orden de la permutación τ del ejemplo 7.1.10 (2) es m.c.m.$(3, 2, 2) = 6$ y el orden de la permutación σ del ejemplo 7.2.5 es m.c.m.$(3, 4, 4) = 12$.

7.3 El grupo alternado

Observación 7.3.1. Según el corolario 7.2.4 toda permutación $\sigma \in S_n$ se puede escribir como un producto

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s \tag{7.3.1.1}$$

de trasposiciones. Sin embargo esta descomposición no es única. De hecho las descomposiciones de σ como producto de trasposiciones no tienen por qué tener el mismo número de trasposiciones. En efecto, sea σ_{s+1} una trasposición. Como las trasposiciones tienen orden 2, tenemos que σ_{s+1}^2 es la permutación identidad, por lo que multiplicando por σ_{s+1}^2 ambos lados de (7.3.1.1) obtenemos

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s\sigma_{s+1}\sigma_{s+1},$$

que, obviamente, es una descomposión distinta a (7.3.1.1) y consiste en el producto de $s + 2$ trasposiciones mientras que (7.3.1.1) consiste en el producto de s trasposiciones.

Aunque según acabamos de ver en la observación 7.3.1 la descomposición de una permutación σ como producto de trasposiciones no es única, lo que no varía es la *paridad* del número de trasposiciones necesarias para descomponer σ. Para demostrar esto vemos primero que la permutación identidad solo se puede escribir como producto de un número par de trasposiciones:

Lema 7.3.2. *Si* $\mathrm{id} \in S_n$ *es un producto*

$$\mathrm{id} = \sigma_1\sigma_2\cdots\sigma_k$$

de k trasposiciones $\sigma_1, \sigma_2, \ldots, \sigma_k$ de S_n, entonces k es par.

Demostración. Consideramos el producto

$$P = \prod_{i<j}(i - j),$$

donde $i, j \in \{1, 2, \ldots, n\}$. Dada $\sigma \in S_n$, definimos σP como el producto

$$\sigma P = \prod_{i<j} (\sigma(i) - \sigma(j)),$$

donde $i, j \in \{1, 2, \ldots, n\}$. Si σ es una trasposición, una comprobación rutinaria muestra que $\sigma P = -P$ (para más detalles, puedes ver la demostración de la proposición III.2.4 de *Álgebra lineal y geometría*, de M. Castellet e I. Llerena). Si aplicamos a P de manera sucesiva las trasposiciones $\sigma_k, \sigma_{k-1}, \ldots, \sigma_2, \sigma_1$ obtendremos $(-1)^k P$. Por otra parte, como $\mathrm{id} = \sigma_1 \sigma_2 \cdots \sigma_k$, el resultado de aplicar a P de manera sucesiva las trasposiciones $\sigma_k, \sigma_{k-1}, \ldots, \sigma_2, \sigma_1$ deber ser P, por lo que $P = (-1)^k P$, y como P es un entero no nulo, $(-1)^k = 1$, de donde k es par. □

Proposición 7.3.3. *Sea $\rho \in S_n$. Sean $\sigma_1, \sigma_2, \ldots, \sigma_k$, $\tau_1, \tau_2, \ldots, \tau_l$ trasposiciones de S_n tales que*

$$\rho = \sigma_1 \sigma_2 \cdots \sigma_k = \tau_1 \tau_2 \cdots \tau_l. \tag{7.3.3.1}$$

Entonces k y l tienen la misma paridad. Por tanto,

- *si ρ se escribe como producto de un número par de trasposiciones, el número de trasposiciones en cualquier descomposición de ρ como producto de trasposiciones es par;*
- *si ρ se escribe como producto de un número impar de trasposiciones, el número de trasposiciones en cualquier descomposición de ρ como producto de trasposiciones es impar.*

En particular ρ no puede descomponerse como producto de un número par y de un número impar de trasposiciones.

Demostración. Como una trasposición tiene orden 2, (7.3.3.1) implica

$$\mathrm{id} = \sigma_1 \sigma_2 \cdots \sigma_k \tau_l \cdots \tau_2 \tau_1.$$

El lema 7.3.2 nos dice que $k + l$ es par. □

La proposición 7.3.3 nos permite distinguir entre permutaciones *pares* e *impares*:

Definición 7.3.4. Decimos que una permutación es *par* si se descompone como producto de un número par de trasposiciones y que es *impar* si se descompone como producto de un número impar de trasposiciones. Por la proposición 7.3.3, una permutación σ, o bien σ es par, o bien σ es impar.

Observación 7.3.5. Dadas $\sigma, \tau \in S_n$ y sendas descomposiciones de σ y τ

$$\sigma = \sigma_1 \cdots \sigma_s, \ \tau = \tau_1 \cdots \tau_t,$$

como producto de trasposiciones, entonces

$$\sigma\tau = \sigma_1 \cdots \sigma_s \tau_1 \cdots \tau_t.$$

Por tanto, es claro a partir de la definición 7.3.3 que el producto de dos permutaciones pares es par, el producto de dos permutaciones impares es par, y el producto de una permutación par y de otra impar es impar.

Ejemplos 7.3.6. (1) El lema 7.3.2 nos dice que la identidad es una permutación par.

Las proposiciones 7.2.1 y 7.2.3 nos permiten decidir fácilmente si una permutación es par o impar:

(2) Por la proposición 7.2.3, un k-ciclo es par si k es impar y es impar si k es par. En particular, una trasposición es una permutación impar.

(3) La permutación τ del ejemplo 7.1.10 (2) es par, ya que es el producto de un 3-ciclo y dos trasposiciones y, por la proposición 7.2.3, se puede descomponer como producto de 4 trasposiciones.

(4) La permutación σ del ejemplo 7.2.5 es par, ya que, según vimos en el ejemplo 7.2.5 (ii), se puede descomponer como producto de 8 trasposiciones. También podemos argumentar que es par usando la observación 7.3.5, ya que σ es el producto de dos 4-ciclos, que son permutaciones impares y un 3-ciclo, que es una permutación par.

Las permutaciones pares forma un subgrupo normal de S_n, el *grupo alternado*:

Proposición 7.3.7. *El conjunto A_n formado por todas las permutaciones pares de S_n es un subgrupo normal de índice* 2 *de S_n.*

Demostración. Definimos la aplicación Ψ de S_n a $(\{1,-1\},\cdot)$ así: dada $\sigma \in S_n$, $\Psi(\sigma) = 1$ si σ es par y $\Psi(\sigma) = -1$ si σ es impar. La aplicación Ψ es un homomorfismo de grupos sobreyectivo. En efecto, para ver que Ψ es un homomorfismo de grupos, debemos ver que si $\sigma, \tau \in S_n$, entonces $\Psi(\sigma\tau) = \Psi(\sigma)\Psi(\tau)$ y esto se sigue de la observación 7.3.5 y de la definición de Ψ. Además Ψ es sobreyectivo ya que, por el lema 7.3.2, la imagen de la permutación identidad es 1 y la imagen de una trasposición es -1.

Por la definición de Ψ, su núcleo es A_n, que es un subgrupo normal de S_n por la proposición 6.2.5. Por el teorema 6.3.3, S_n/A_n es isomorfo a $\{1,-1\}$, ya que Ψ es sobreyectivo. Como $\{1,-1\}$ tiene 2 elementos, S_n/A_n tiene también dos elementos, es decir, A_n tiene índice 2 en S_n. □

Definición 7.3.8. Al subgrupo A_n se le denomina grupo alternado.

Concluimos la sección enunciando un teorema muy importante, el teorema de Abel, relativo al grupo alternado. No incluimos aquí la demostración; la puedes encontrar en el teorema G.31 de *Galois Theory*, segunda edición, de Joseph Rotman para el caso $n = 5$ o en el teorema III.2.5 de *Estructuras Algebraicas: Teoría Elemental de Grupos*, de J.F. Fernando y J.M. Gamboa.

Teorema 7.3.9. *(Abel) Si $n \geq 5$, los únicos subgrupos normales del grupo alternado a A_n son $< id >$ y A_n.*

Como consecuencia del teorema 7.3.9 (véase por ejemplo el corolario III.2.5 de *Estructuras Algebraicas: Teoría Elemental de Grupos*, de J.F. Fernando y J.M. Gamboa) se demuestra que los únicos subgrupos normales de S_n son $< \mathrm{id} >$, A_n y S_n. Este resultado y, en general, la estructura y los subgrupos de S_n, son cruciales para el estudio de las soluciones de ecuaciones polinómicas en una variable. El corolario que acabamos de mencionar implica que, para cada $n \geq 5$, existen polinomios cuyas raíces no se pueden escribir mediante expresiones radicales de los coeficientes del polinomio (de hecho, si $n \geq 5$, las raíces del polinomio *general* de grado n no se pueden expresar mediante radicales). Por contra, las raíces de cualquier polinomio de grado menor o igual que 4 sí son expresables mediante radicales[2]. El estudio de las soluciones de ecuaciones polinómicas es el tema central de la Teoría de Galois. Este estudio se basa en una conexión muy profunda entre la teoría de grupos y la teoría de extensiones de cuerpos. En el ejemplo 8.1.15 se indica el primer paso de esta conexión.

[2]El ejemplo de raíces expresables mediante radicales que conoces sobradamente es el de las soluciones de una ecuación de segundo grado $aX^2 + bX + c = 0$ con coeficientes en un cuerpo de característica distinta de 2, que son $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$. Según acabamos de mencionar, las soluciones de ecuaciones de tercer y cuarto grado también son expresables mediante radicales, pero esas fórmulas son más complicadas (véase *Galois Theory*, segunda edición, de Joseph Rotman, pp. 44-49).

Tema 8

Acción de un grupo en un conjunto

Aunque en los temas precedentes hemos intentado introducir los grupos de una manera bastante concreta, a veces un grupo G puede aparecer de manera abstracta. Una de las formas de pasar de esa abstracción a un enfoque más concreto es estudiar cómo *G actúa* en diferentes conjuntos. Además, el estudio de la *acción* de un grupo G en un conjunto nos da información sobre la estructura de G (véase el corolario 8.3.5 y los ejercicios 10 y 11, que podemos ver como una aplicación sencilla a la cristalografía). Así, las acciones de grupos se utilizan por ejemplo para demostrar los *teoremas de Sylow* (que no veremos en este curso), que sirven a su vez para profundizar en la estructura de los grupos finitos. Esto a su vez tiene gran relevancia para la *Teoría de Galois*.

8.1 Definiciones y ejemplos

Definición 8.1.1. Sea G un grupo y sea X un conjunto no vacío.

(1) Una *acción por la izquierda* de G en X es una aplicación

$$\begin{array}{rccc} \alpha: & G \times X & \longrightarrow & X \\ & (g,x) & \mapsto & gx, \end{array}$$

(donde gx es simplemente una notación; es la forma en que denotamos $\alpha(g,x)$, es decir, $gx := \alpha(g,x)$), que, para todo $x \in X$, cumple:

(a) $(g_1 \cdot g_2)x = g_1(g_2x)$, para todo $g_1, g_2 \in G$ (donde el signo $\cdot$, que normalmente obviaremos, en el paréntesis de la izquierda es el producto en G);

(b) $1_G x = x$.

Cuando existe una acción por la izquierda de G en X decimos que *G actúa por la izquierda* en X.

(2) Una *acción por la derecha*

$$\begin{array}{rccc} \beta: & X \times G & \longrightarrow & X \\ & (x, g) & \mapsto & xg, \end{array}$$

(donde xg es simplemente una notación; es la forma en que denotamos $\beta(x, g)$, es decir, $xg := \beta(x, g)$), que, para todo $x \in X$, cumple:

(a') $x(g_1 \cdot g_2) = (xg_1)g_2$, para todo $g_1, g_2 \in G$ (donde el signo $\cdot$, que normalmente obviaremos, en el paréntesis de la izquierda es el producto en G);

(b') $x1_G = x$.

Cuando existe una acción por la derecha de G en X decimos que G *actúa por la derecha* en X.

Observación 8.1.2. (1) La diferencia entre una acción por la izquierda y una acción por la derecha está en las propiedades (a) y (a'), es decir, en el orden en que actúan los factores de un producto g_1g_2 sobre los elementos de X (en el caso de una acción por la izquierda g_2 actúa primero y en el caso de una acción por la derecha g_1 actúa primero). Por tanto, los conceptos de acción por la izquierda y por la derecha son distintos si G no es abeliano.

(2) Una acción

$$\begin{array}{rccc} \alpha: & G \times X & \longrightarrow & X \\ & (g, x) & \mapsto & gx \end{array}$$

por la izquierda da lugar a la siguiente acción por la derecha:

$$\begin{array}{rccc} \alpha': & X \times G & \longrightarrow & X \\ & (x, g) & \mapsto & xg := g^{-1}x. \end{array}$$

En efecto, α' es una acción por la derecha porque $x(g_1g_2) := (g_1g_2)^{-1}x = (g_2^{-1}g_1^{-1})x = g_2^{-1}(g_1^{-1}x)$ y $(xg_1)g_2 := g_2^{-1}(g_1^{-1}x)$. Recíprocamente, una acción

$$\begin{array}{rccc} \beta: & X \times G & \longrightarrow & X \\ & (x, g) & \mapsto & xg, \end{array}$$

por la derecha da lugar a la siguiente acción por la izquierda:

$$\begin{array}{rccc} \beta': & G \times X & \longrightarrow & X \\ & (g, x) & \mapsto & gx := xg^{-1}. \end{array}$$

Es claro que las maneras que acabamos de describir de asignar a cada acción por la izquierda una acción por la derecha y de asignar a cada acción por la derecha una acción por la izquierda son inversas una de la otra así que nos permiten establecer una biyección entre el conjunto de acciones por la izquierda y el conjunto de acciones por la derecha de un grupo G en un conjunto X. Por ello es suficiente estudiar solamente las acciones por la izquierda y eso es lo que haremos. Así pues, a partir de ahora y a no ser que se diga explícitamente otra cosa, una acción será una acción por la izquierda.

Observación 8.1.3. Sea G un grupo y sea H un subgrupo de G. Una acción de G en un conjunto X se restringe a una acción de H en X de la manera obvia.

Proposición 8.1.4. *Sea G un grupo y sea X un conjunto no vacío. Sea $\mathrm{Acc}(G,X)$ el conjunto de acciones de G en X y sea $\mathrm{Hom}(G,\mathrm{Biy}(X))$ el conjunto de homomorfismos de grupos de G a $(\mathrm{Biy}(X),\circ)$. La aplicación*

$$\begin{array}{rccc} \Phi: & \mathrm{Acc}(G,X) & \longrightarrow & \mathrm{Hom}(G,\mathrm{Biy}(X)) \\ & \alpha & \mapsto & \rho, \end{array}$$

donde

$$\begin{array}{rccc} \alpha: & G\times X & \longrightarrow & X \\ & (g,x) & \mapsto & gx, \end{array}$$

y, para todo $g\in G$,

$$\begin{array}{rccc} \rho(g): & X & \longrightarrow & X \\ & x & \mapsto & gx \end{array}$$

y la aplicación

$$\begin{array}{rccc} \Psi: & \mathrm{Hom}(G,\mathrm{Biy}(X)) & \longrightarrow & \mathrm{Acc}(G,X) \\ & \vartheta & \mapsto & \varepsilon, \end{array}$$

donde

$$\begin{array}{rccc} \varepsilon: & G\times X & \longrightarrow & X \\ & (g,x) & \mapsto & \vartheta(g)(x), \end{array}$$

son biyectivas e inversas una de la otra. Por tanto existe una biyección entre los conjuntos $\mathrm{Acc}(G,X)$ y $\mathrm{Hom}(G,\mathrm{Biy}(X))$.

Demostración. Vemos primero que Φ es una aplicación entre $\mathrm{Acc}(G,X)$ y $\mathrm{Hom}(G,\mathrm{Biy}(X))$. Para ello vemos que ρ es, en efecto, un homomorfismo de grupos entre G y $(\mathrm{Biy}(X),\circ)$. Comprobamos en primer lugar que ρ es una aplicación entre G y $(\mathrm{Biy}(X),\circ)$. Para ello vemos que $\rho(g)$ es una aplicación biyectiva de X en X. Por una parte $\rho(g)$ es una aplicación de X en X, ya que $\rho(g)(x)=gx\in X$, puesto que α es una acción de G en X. Por otra parte la aplicación $\rho(g^{-1})$ es la inversa de $\rho(g)$, ya que $(\rho(g^{-1})\circ\rho(g))(x)=g^{-1}(gx)=(g^{-1}g)x=1_Gx=x$ y $(\rho(g)\circ\rho(g^{-1}))(x)=g(g^{-1}x)=(gg^{-1})x=1_Gx=x$. Así pues, $\rho(g)$ es una aplicación biyectiva de X en X.

Vemos ahora que ρ es homomorfismo de grupos. En efecto, tenemos que

$$\begin{array}{rccc} \rho(g_1g_2): & X & \longrightarrow & X \\ & x & \mapsto & (g_1g_2)x \end{array}$$

y

$$\begin{array}{rccc} \rho(g_1)\circ\rho(g_2): & X & \longrightarrow & X \\ & x & \mapsto & g_1(g_2x). \end{array}$$

Como $(g_1g_2)x=g_1(g_2x)$ para todo $x\in X$ y para todo $g_1,g_2\in G$, concluimos que $\rho(g_1g_2)=\rho(g_1)\circ\rho(g_2)$.

En segundo lugar comprobamos que Ψ es una aplicación entre $\mathrm{Hom}(G, \mathrm{Biy}(X))$ y $\mathrm{Acc}(G, X)$. Para ello tenemos que ver que ε es una acción de G en X. Vemos en primer lugar que ε es una aplicación de $G \times X$ en X. En efecto, $\varepsilon(g, x) := \vartheta(g)(x)$ y $\vartheta(g)(x)$ pertenece a X, ya que ϑ es un homomorfismo de G en $\mathrm{Biy}(X)$, por lo que, para todo $g \in G$, $\vartheta(g)$ es una aplicación biyectiva de X en X. Comprobamos ahora que ε cumple las propiedades (a) y (b) de la definición 8.1.1. Para ello usamos que ϑ es un homomorfismo. La propiedad (a) se cumple porque $\vartheta(g_1 g_2)(x) = (\vartheta(g_1) \circ \vartheta(g_2))(x) = \vartheta(g_1)(\vartheta(g_2)(x))$. La propiedad (b) se cumple porque $\vartheta(1_G)(x) = \mathrm{id}(x) = x$.

Finalmente comprobamos que Φ y Ψ son aplicaciones inversas una de la otra. A la acción

$$\begin{array}{rccc} \alpha: & G \times X & \longrightarrow & X \\ & (g, x) & \mapsto & gx, \end{array}$$

la aplicación Φ le hace corresponder el homomorfismo de grupos ρ entre G y $(\mathrm{Biy}(X), \circ)$, donde, para todo $g \in G$,

$$\begin{array}{rccc} \rho(g): & X & \longrightarrow & X \\ & x & \mapsto & gx \end{array}$$

y, a ρ, la aplicación Ψ le hace corresponder la acción

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \mapsto & \rho(g)(x) = gx, \end{array}$$

que es la acción α con la que habíamos comenzado.

Dado ahora un homomorfismo de grupos ϑ entre G y $(\mathrm{Biy}(X), \circ)$, la aplicación Ψ le hace corresponder la acción

$$\begin{array}{rccc} \varepsilon: & G \times X & \longrightarrow & X \\ & (g, x) & \mapsto & \vartheta(g)(x) \end{array}$$

y, a la acción ε, la aplicación Φ le hace corresponder el homomorfismo que envía cada $g \in G$ a la aplicación biyectiva

$$\begin{array}{ccc} X & \longrightarrow & X \\ x & \mapsto & \varepsilon(g, x) = \vartheta(g)(x); \end{array}$$

este es el homomorfismo ϑ con el que habíamos comenzado. □

Observación 8.1.5. A partir de ahora cuando hablemos de una acción nos referiremos indistintamente a una acción α tal como se definió en la definición 8.1.1 (1) o al homomorfismo de grupos $\Phi(\alpha)$ definido en la proposición 8.1.4.

Ejemplo 8.1.6. Sea G un grupo y sea X un conjunto no vacío. Entonces

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \mapsto & x, \end{array}$$

es una acción de G en X y se denomina la acción *trivial* de G en X. Una acción es trivial si y solo si la aplicación Φ de la proposición 8.1.4 le hace corresponder el homomorfismo de grupos constante, es decir, el homomorfismo de grupos que envía cada g de G a id_X.

Ejemplos 8.1.7. Sea G un grupo.

(1) El grupo G actúa (por la izquierda) en G de la siguiente forma:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, g') & \mapsto & g \cdot g', \end{array}$$

donde $\cdot$ es el producto en G, G juega el papel de grupo en el primer factor del producto cartesiano y G juega el papel de conjunto X en el segundo factor del producto cartesiano y en el conjunto final de la aplicación.

(2) Si en (1) intercambiamos los papeles de G como grupo y como conjunto, la aplicación descrita en (1) es una acción por la derecha de G en G.

(3) El grupo G actúa en G por *conjugación* de la siguiente manera:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, g') & \mapsto & g \cdot g' \cdot g^{-1}, \end{array}$$

donde $\cdot$ es el producto en G, G juega el papel de grupo en el primer factor del producto cartesiano y G juega el papel de conjunto X en el segundo factor del producto cartesiano y en el conjunto final de la aplicación.

Ejemplos 8.1.8. (1) El grupo diédrico D_n actúa en el polígono regular de n lados P_n (entendemos que P_n es el conjunto de puntos que están en los lados del polígono, aunque D_n también actúa en la región del plano delimitada por ese conjunto de puntos), de la manera obvia: dados $\sigma \in D_n$ y $x \in P_n$, definimos σx como $\sigma(x)$.

(2) El grupo diédrico D_n actúa en el conjunto formado por los vértices de P_n de la manera obvia: dados $\sigma \in D_n$ y p un vértice de P_n, definimos σp como $\sigma(p)$. Numerando de 1 a n los vértices de P_n obtenemos una acción de D_n en el conjunto $\{1, 2, \ldots, n\}$. Entonces, por la proposición 8.1.4, tenemos un homomorfismo de D_n en S_n (compárese con los ejercicios 3 y 4 del tema 6). Esta acción y este homomorfismo no son canónicos pues dependen de la forma en que hayamos numerado los vértices de P_n.

Ejemplos 8.1.9. Sea $\mathbf{k}$ un cuerpo.

(1) El grupo general lineal $GL(n, \mathbf{k})$ actúa (por la izquierda) en $\mathbf{k}^n$ y en $\mathbf{k}^n \setminus \{(0, 0, \ldots, 0)\}$ de la siguiente manera: para toda $M \in GL(n, \mathbf{k})$ y para todo v de $\mathbf{k}^n$, definimos la acción de M en v como $(M \cdot v^t)^t$, donde $\cdot$ es el producto de matrices. Observa que definiendo la acción de M en v como $v \cdot M$ obtenemos una acción por la derecha de $GL(n, \mathbf{k})$ en $\mathbf{k}^n$ y en $\mathbf{k}^n \setminus \{(0, 0, \ldots, 0)\}$.

(2) La acción de $GL(n, \mathbf{k})$ en $\mathbf{k}^n$ y en $\mathbf{k}^n \setminus \{(0, 0, \ldots, 0)\}$ descrita en (1) se restringe, por la observación 8.1.3, a acciones del grupo especial lineal $SL(n, \mathbf{k})$ en $\mathbf{k}^n$ y en $\mathbf{k}^n \setminus \{(0, 0, \ldots, 0)\}$.

(3) La acción de $GL(n, \mathbf{R})$ en $\mathbf{R}^n$ y en $\mathbf{R}^n \setminus \{(0, 0, \ldots, 0)\}$ también se restringe a acciones de los grupos ortogonal $O(n)$ y especial ortogonal $SO(n)$.

Ejemplos 8.1.10. Sea V un espacio vectorial de dimensión n sobre un cuerpo $\mathbf{k}$ (por ejemplo $V = \mathbf{k}^n$).

(1) El grupo general lineal $GL(V)$ actúa en V ya que $GL(V)$ es un subgrupo de $\mathrm{Biy}(V)$. Además, los isomorfismos dados en el ejemplo 6.1.22 definen acciones de $GL(\mathbf{k}, n)$ en V.

(2) Si V es un espacio vectorial euclídeo de dimensión n, entonces el grupo ortogonal $O(V)$ y el grupo especial ortogonal $SO(V)$ actúan en V ya que son subgrupos de $\mathrm{Biy}(V)$. Además, los isomorfismos dados en el ejemplo 6.1.23 definen acciones de $O(n)$ y $SO(n)$ en V.

Ejemplos 8.1.11. Sea V de nuevo un espacio vectorial de dimensión n sobre un cuerpo $\mathbf{k}$

(1) El grupo multiplicativo $\mathbf{k}^*$ de las unidades de $\mathbf{k}$ actúa en $V \setminus \{\vec{0}\}$ de la siguiente manera: para todo $\lambda \in \mathbf{k}^*$ y todo $v \in V \setminus \{\vec{0}\}$, la acción de λ en v es $\lambda \cdot v$, donde $\cdot$ es el producto por escalares de V.

(2) Si $\mathbf{k} = \mathbf{R}$, como consecuencia de (3) y de la observación 8.1.3, el subgrupo $\mathbf{R}^+ := \{x \in \mathbf{R} \mid x > 0\}$ de $\mathbf{R}^*$ actúa en $V \setminus \{\vec{0}\}$.

(3) El subgrupo $< -1 >$ de $\mathbf{R}^*$ actúa en la esfera $\mathbf{S}^{n-1} := \{(x_1, \ldots, x_n) \in \mathbf{R}^n \mid x_1^2 + \cdots + x_n^2 = 1\}$ de la siguiente manera: dado n de $< -1 >$ y v de $\mathbf{S}^{n-1}$, la acción de n en v es $n \cdot v$, donde $\cdot$ es el producto por escalares en $\mathbf{R}^n$.

Ejemplo 8.1.12. Sea $\mathbf{k}$ un cuerpo.

(1) El grupo general lineal $GL(\mathbf{k}, n+1)$ actúa en el espacio proyectivo $\mathbf{P}^n_{\mathbf{k}}$ de la forma que se indica a continuación. Sea $M \in GL(\mathbf{k}, n+1)$; dado $v = (a_0, a_1, \ldots, a_n) \in \mathbf{k}^{n+1}$, si denotamos el punto $(a_0 : a_1 : \cdots : a_n)$ de $\mathbf{P}^n_{\mathbf{k}}$ como $[v]$, M actúa (por la izquierda) en $[v]$ como $M[v] := [(Mv^t)^t]$. En efecto, al ser $\mathbf{P}^n_{\mathbf{k}}$ un conjunto cociente (véase el ejemplo 8.2.10 (8)), hay que comprobar que la acción está bien definida pero eso es así ya que, dado $\lambda \in \mathbf{k}^*$ y dada w una matriz $n \times 1$ con coeficientes en $\mathbf{k}$, $M\lambda w = \lambda M w$. Que en efecto es una acción se sigue del ejemplo 8.1.9.

(2) La acción de $GL(n+1, \mathbf{k})$ en $\mathbf{P}^n_{\mathbf{k}}$ descrita en (1) se restringe, por la observación 8.1.3, a una acción del grupo especial lineal $SL(n, \mathbf{k})$ en $\mathbf{P}^n_{\mathbf{k}}$.

(3) La acción de $GL(n+1, \mathbf{R})$ en $\mathbf{P}^n_{\mathbf{R}}$ también se restringe a acciones de los grupos ortogonal $O(n)$ y especial ortogonal $SO(n)$ en $\mathbf{P}^n_{\mathbf{R}}$.

(4) De manera análoga, si V es un espacio vectorial sobre $\mathbf{k}$ de dimensión finita, los grupos $GL(V)$ y $SL(V)$ actúan en $\mathbf{P}(V)$ (la proyectivización de V, véase el ejemplo 8.2.10 (8)) y, si V es un espacio vectorial euclídeo de dimensión finita, los grupos $O(V)$ y $SO(V)$ actúan en $\mathbf{P}(V)$.

Ejemplos 8.1.13. Sea A un espacio afín de dimensión n sobre un cuerpo $\mathbf{k}$ y sea V su espacio vectorial asociado.

(1) El grupo aditivo $(V, +)$ del espacio vectorial V actúa en A así:

$$\begin{array}{ccc} V \times A & \longrightarrow & A \\ (v, p) & \mapsto & p + v. \end{array}$$

(2) Si $\mathbf{k} = \mathbf{R}$ y A es el espacio afín estándar $\mathbf{A}^n_{\mathbf{R}}$, la acción descrita en (1) se restringe a una acción del grupo $(\mathbf{Z}^n, +)$ en $\mathbf{R}^n$.

Ejemplo 8.1.14. El grupo $(\mathbf{R}, +)$ actúa en $\mathbf{C}$ así:

$$\begin{array}{ccc} \mathbf{R} \times \mathbf{C} & \longrightarrow & \mathbf{C} \\ (\theta, z) & \mapsto & e^{2\theta\pi i} z. \end{array}$$

¿Qué relación hay entre esta acción y la de $SO(2)$ en $\mathbf{R}^2$ descrita en el ejemplo 8.1.9 (2)?

Ejemplo 8.1.15. Sea $\mathbf{k}$ un cuerpo, sea $f(X)$ un polinomio de $\mathbf{k}[X]$ de grado n y sea K un cuerpo que cumple

(i) $\mathbf{k}$ es un subanillo unitario de K;

(ii) $f(X)$ factoriza como producto de polinomios de $K[X]$ de grado 1;

(iii) K es el cuerpo "más pequeño" que cumple (i) y (ii), es decir, si K' es un cuerpo que cumple (i) y (ii) tal que K' es un subanillo unitario de K, entonces $K' = K$.[1]

Un *automorfismo* de la *extensión* $\mathbf{k} \subset K$ es un isomorfismo φ de K en K tal que $\varphi(\lambda) = \lambda$ para todo λ de $\mathbf{k}$. Los automorfismos de $\mathbf{k} \subset K$ forman un grupo, que recibe el nombre de *grupo de Galois* de f y se denota $\mathrm{Gal}(K/\mathbf{k})$. El grupo $\mathrm{Gal}(K/\mathbf{k})$ actúa en el conjunto de raíces de f en K. Si f tiene n raíces (distintas) en K,[2] numerándolas del 1 al n, tenemos, por la proposición 8.1.4, un homomorfismo de grupos de $\mathrm{Gal}(K/\mathbf{k})$ a S_n.[3]

[1] A K se le denomina *cuerpo de descomposición* de f. El cuerpo de descomposición de f es el "cuerpo más pequeño" que contiene a todas sus raíces.

[2] Se dice en ese caso que f es *separable*. Esto ocurre por ejemplo si f es irreducible en $\mathbf{k}[X]$ y $\mathbf{k}$ tiene característica 0 o $\mathbf{k}$ es finito.

[3] Se puede demostrar que un elemento de $\mathrm{Gal}(K/\mathbf{k})$ está determinado de forma única por el valor que toma en las raíces de f en K. Esto implica que el homomorfismo de $\mathrm{Gal}(K/\mathbf{k})$ a S_n es inyectivo y, por tanto, que $\mathrm{Gal}(K/\mathbf{k})$ es isomorfo a un subgrupo de S_n. El estudio del grupo de f está en el centro de la teoría de Galois y nos dice entre otras cosas en qué casos f es resoluble por radicales. La teoría de Galois implica que, por ser el grupo de Galois de un polinomio f (irreducible y separable) de grado 4 isomorfo a un subgrupo de S_4, el polinomio f es resoluble por radicales. En cambio, la teoría de Galois también implica que, al ser A_5 simple (véase el teorema 7.3.9), los polinomios (irreducibles y separables) de grado 5 cuyo grupo de Galois es isomorfo a S_5 o A_5 no son resolubles por radicales.

8.2 Órbitas de una acción

Observación 8.2.1. Sea

$$\begin{array}{rccc} \alpha: & G\times X & \longrightarrow & X \\ & (g,x) & \mapsto & gx \end{array}$$

una acción de un grupo G en un conjunto X. La acción α determina la siguiente relación de equivalencia $\sim$ en X: para cualesquiera $x_1, x_2 \in X$, $x_1 \sim x_2$ si y solo si existe $g \in G$ tal que $x_2 = gx_1$.

Comprobamos que, en efecto, la relación $\sim$ cumple las propiedades reflexiva, simétrica y transitiva. La propiedad reflexiva se cumple ya que $1_G x = x$. La propiedad simétrica se cumple pues, si $x_2 = gx_1$, entonces $x_1 = 1_G x_1 = (g^{-1}g)x_1 = g^{-1}(gx_1) = g^{-1}x_2$. Finalmente, la propiedad transitiva se cumple pues, si $x_2 = gx_1$ y $x_3 = g'x_2$, entonces $x_3 = g'x_2 = g'(gx_1) = (g'g)x_1$.

Definición 8.2.2. Sea

$$\begin{array}{rccc} \alpha: & G\times X & \longrightarrow & X \\ & (g,x) & \mapsto & gx \end{array}$$

una acción de un grupo G en un conjunto X.

(1) A las clases de equivalencia de la relación $\sim$ definida por α se las denomina *órbitas* de la acción. Dado $x \in X$, la órbita de x se denota Gx u $\mathrm{Orb}(x)$ y es

$$\mathrm{Orb}(x) = Gx := \{gx \mid g \in G\}.$$

(2) Al conjunto cociente $X/\sim$ lo denotaremos normalmente X/G. Por tanto X/G es el conjunto de las órbitas de α.

(3) Dado $x \in X$ definimos el *estabilizador* de x, que denotamos como G_x o $\mathrm{Stab}(x)$, como el conjunto

$$G_x = \mathrm{Stab}(x) := \{g \in G \mid gx = x\}.$$

Decimos que x es un *punto fijo* de α si $\mathrm{Stab}(x) = G$, es decir, si para todo $g \in G$ se tiene $gx = x$, es decir, si $Gx = \{x\}$.

Observación 8.2.3. Si un grupo G actúa en un conjunto X y X' es una unión de órbitas de esa acción, la acción de G en X se restringe a una acción de G en X'.

Proposición 8.2.4. *Sea G un grupo que actúa en un conjunto X y sea $x \in X$. El estabilizador de x es un subgrupo de G.*

Demostración. Si $g_1, g_2 \in \mathrm{Stab}(x)$, entonces $(g_1g_2)x = g_1(g_2x) = g_1x = x$, por lo que $g_1g_2 \in \mathrm{Stab}(x)$. Por otra parte, si $g \in \mathrm{Stab}(x)$, entonces $g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = 1_G x = x$, por lo que $g^{-1} \in \mathrm{Stab}(x)$. □

Ejemplo 8.2.5. Consideramos la acción, descrita en el ejemplo 8.1.8 (2), de D_n en el conjunto de vértices de un polígono regular P_n. Sea p un vértice de P_n. El estabilizador de p está formado por la identidad y por la simetría axial de D_n cuyo eje pasa por p.

Definición 8.2.6. Sea

$$\begin{array}{rccc} \alpha: & G\times X & \longrightarrow & X \\ & (g,x) & \mapsto & gx \end{array}$$

una acción de un grupo G en un conjunto X. Decimos que α es

(1) *efectiva* o *fiel* si el homomorfismo de grupos $\Phi(\alpha)$ de la proposición 8.1.4 es inyectivo;

(2) *transitiva* si α tiene solo una órbita, es decir, si para cualesquiera $x, x' \in X$ existe $g \in G$ tal que $x' = gx$.

(3) *libre* o *sin puntos fijos* si α no tiene puntos fijos, es decir, si α no tiene ninguna órbita formada por un solo elemento o, lo que es lo mismo, no existe $x \in X$ tal que $\mathrm{Stab}(x) = G$.

Observación 8.2.7. Si X tiene más de un elemento, una acción transitiva de un grupo G en X es libre.

Estudiaremos a continuación si las acciones presentadas en los ejemplos 8.1.6, 8.1.7, 8.1.8, 8.1.9, 8.1.10, 8.1.11, 8.1.13 y 8.1.14 encajan en los tipos descritos en la definición 8.2.6. Calcularemos también sus órbitas. Nos detenemos en primer lugar en las propiedades de la acción de G en G del ejemplo 8.1.7 (1), ya que de su carácter efectivo deduciremos el teorema de Cayley:

Proposición 8.2.8. *Sea $(G,\cdot)$ un grupo y sea α la acción de G en G descrita en el ejemplo 8.1.7 (1), es decir, sea*

$$\begin{array}{rccc} \alpha: & G\times G & \longrightarrow & G \\ & (g,g') & \mapsto & g\cdot g'. \end{array}$$

(1) La acción α es fiel, es decir, dada la aplicación Φ de la proposición 8.1.4, el homomorfismo de grupos

$$\begin{array}{rccc} \Phi(\alpha): & (G,\cdot) & \longrightarrow & (\mathrm{Biy}(G),\circ) \\ & g & \mapsto & \Phi(\alpha)(g), \end{array}$$

donde

$$\begin{array}{rccc} \Phi(\alpha)(g): & G & \longrightarrow & G \\ & g' & \mapsto & g\cdot g', \end{array}$$

es un homomorfismo inyectivo.

(2) La acción α es transitiva.

(3) Si $G \neq <1>$, la acción α es libre.

Demostración. Vemos que el núcleo de $\Phi(\alpha)$ $=< 1_{_G} >$. En efecto, sea $g \in G$ tal que $\Phi(\alpha)(g) = \mathrm{id}_G$. Entonces aplicando $\Phi(\alpha)(g)$ al elemento 1_G obtenemos $g \cdot 1_G = \mathrm{id}_G(1_G) = 1_G$, de donde $g = 1_G$. Esto prueba que $\Phi(\alpha)$ es un homomorfismo inyectivo.

Para cualesquiera $g', g'' \in G$, definimos $g := g'' \cdot g'^{-1}$. Entonces $g'' = g \cdot g'$. Esto prueba que α tiene una única órbita, que es G; por tanto, α es transitiva. Como la única órbita de α es G, si G tiene más de un elemento entonces α es libre. □

Corolario 8.2.9. *Sea* $(G, \cdot)$ *un grupo.*

(1) El grupo $(G, \cdot)$ *es isomorfo a un subgrupo de* $(\mathrm{Biy}(G), \circ)$.

(2) (Cayley) En particular, si G es un grupo finito de orden n, entonces G es isomorfo a un subgrupo de S_n.

Demostración. El apartado (1) es consecuencia inmediata de la proposición 8.2.8, ya que, al ser $\Phi(\alpha)$ un homomorfismo inyectivo, $(G, \cdot)$ es isomorfo a la imagen de $\Phi(\alpha)$, que es un subgrupo de $(\mathrm{Biy}(G), \circ)$. El apartado (2) se sigue de manera inmediata del apartado (1) y de la observación 7.1.2 (1). □

Ejemplos 8.2.10. (1) Sea α la acción trivial definida en el ejemplo 8.1.6. El núcleo de $\Phi(\alpha)$ es G; por tanto α es fiel si y solo si $G =< 1 >$. Para todo $x \in X$, la órbita de x es $Gx = \{x\}$, por lo cual el conjunto de puntos fijos de la acción trivial es X.

(2) Sea α la acción del ejemplo 8.1.7 (3). El núcleo del homomorfismo de grupos $\Phi(\alpha)$ definido en la proposición 8.1.4 es el conjunto de aquellos elementos de G que conmutan con todos los elementos de G, es decir, el núcleo es el centro de G

$$Z(G) = \{g \in G \mid gg' = g'g \text{ para todo } g' \in G\}$$

que se definió en el ejercicio 16 del tema 6. Por tanto α es fiel si y solo si $Z(G) =< 1_{_G} >$. En el otro extremo, $Z(G) = G$ si y solo si G es abeliano. Por ello, si G es abeliano, entonces la acción α es la acción trivial.

La órbita de un elemento g' de G es su *clase de conjugación*, es decir, el conjunto $\{gg'g^{-1}$ para todo $g \in G\}$. En general α no es transitiva. Si G es abeliano la órbita de cualquier elemento g' de G es $\{g'\}$ (recordemos que, si G es abeliano, entonces la acción α es la acción trivial).

Los puntos fijos de α son aquellos elementos de g' de G que conmutan con todos los elementos de G, es decir, el conjunto de puntos fijos de α es $Z(G)$. Por tanto α es libre si y solo si $Z(G) =< 1_{_G} >$.

(3) Las acciones del ejemplo 8.1.8 son fieles, libres y la del ejemplo 8.1.8 (2) es transitiva. Por el ejemplo 8.1.8 (2) tenemos que D_n se puede identificar, de manera no única, con un subgrupo de S_n (compárese con el ejercicio 4 del tema 6).

(4) Las acciones de los ejemplos 8.1.9 (1) y (2) en $\mathbf{k}^n$ y la acción del ejemplo 8.1.10 (1) en V son fieles (puesto que $GL(n,\mathbf{k})$ y $SL(n,\mathbf{k})$ son subgrupos de $\mathrm{Biy}(\mathbf{k}^n)$ y $GL(V)$ es subgrupo de $\mathrm{Biy}(V)$). Todas ellas tienen dos órbitas, que son los conjuntos $\{(0,0,\ldots,0)\}$ y $\mathbf{k}^n \smallsetminus \{(0,0,\ldots,0)\}$ en los dos primeros ejemplos y los conjuntos $\{\vec{0}\}$ y $V \smallsetminus \{\vec{0}\}$ en el tercer ejemplo. Por ello, las acciones de los ejemplos 8.1.9 (1) y (2) en $\mathbf{k}^n \smallsetminus \{(0,0,\ldots,0)\}$ y la acción del ejemplo 8.1.10 (1) en $V \smallsetminus \{\vec{0}\}$ (véase la observación 8.2.3) son transitivas. El único punto fijo de estas acciones es el vector $(0,0,\ldots,0)$ en los dos primeros ejemplos y el vector $\vec{0}$ en el tercero, por lo que las acciones de los ejemplos 8.1.9 (1) y (2) en $\mathbf{k}^n \smallsetminus \{(0,0,\ldots,0)\}$ y la acción del ejemplo 8.1.10 (1) en $V \smallsetminus \{\vec{0}\}$ son libres.

(5) Como en (4), las acciones del ejemplo 8.1.9 (3) en $\mathbf{R}^n$ y las acciones del ejemplo 8.1.10 (2) en V son fieles y tienen un único punto fijo ($(0,0,\ldots,0)$ y $\vec{0}$ en cada caso), por lo que sus restricciones a $\mathbf{R}^n \smallsetminus \{(0,0,\ldots,0)\}$ y $V \smallsetminus \{\vec{0}\}$ son libres. En cambio estas acciones tienen infinitas órbitas. Las órbitas de las acciones del ejemplo 8.1.9 (3) son el conjunto $\{(0,0,\ldots,0)\}$ y las esferas de $\mathbf{R}^n$ de centro $(0,\ldots,0)$ y radio positivo. Análogamente, las órbitas de las acciones del ejemplo 8.1.10 (2) son $\{0\}$ y, para cada $r \in \mathbf{R}, r > 0$, el conjunto $\{v \in V \mid \|v\| = r\}$.

(6) La acción α del ejemplo 8.1.11 (1) es fiel y libre. La imagen de $\Phi(\alpha)$ en $\mathrm{Biy}(V)$ es el grupo formado por la identidad y las homotecias vectoriales. Las órbitas de α son las rectas vectoriales de V sin el vector $\vec{0}$. El cociente $\frac{V \smallsetminus \{\vec{0}\}}{\mathbf{k}^*}$ es una de las construcciones que se toma como definición del espacio proyectivo $\mathbf{P}(V)$.

(7) La acción α del ejemplo 8.1.11 (2) es fiel y libre. La imagen de $\Phi(\alpha)$ en $\mathrm{Biy}(\mathbf{R}^n)$ es el grupo formado por la identidad y las homotecias vectoriales de razón positiva. Las órbitas de α son las semirectas vectoriales de $\mathbf{R}^n$ (sin el vector $\vec{0}$). El cociente $\mathbf{R}^n/\mathbf{R}^+$ se puede identificar de manera natural con la esfera $\mathbf{S}^{n-1} := \{(x_1,\ldots,x_n) \in \mathbf{R}^n \mid x_1^2 + \cdots + x_n^2 = 1\}$.

(8) La acción del ejemplo 8.1.11 (3) es fiel y libre. Sus órbitas son los pares de puntos antipodales de la esfera $\mathbf{S}^{n-1}$. Por tanto, el cociente $\mathbf{S}^{n-1}/<-1>$ y el cociente $\frac{\mathbf{R}^n \smallsetminus \{\vec{0}\}}{\mathbf{R}^*}$ se pueden identificar de manera natural. Por ello $\mathbf{S}^{n-1}/<-1>$ se puede tomar como modelo del espacio proyectivo $\mathbf{P}^{n-1}_{\mathbf{R}}$. Trata de usar este modelo para visualizar $\mathbf{P}^2_{\mathbf{R}}$.

(9) La acción α del ejemplo 8.1.13 (1) es fiel, transitiva y libre. La imagen de $\Phi(\alpha)$ en $\mathrm{Biy}(A)$ es el grupo formado por las traslaciones de A.

(10) La acción α del ejemplo 8.1.14 no es fiel ya que el núcleo de $\Phi(\alpha)$ es $\mathbf{Z}$. Tiene un único punto fijo, el 0, por lo cual es libre si la restringimos a $\mathbf{C}^*$. Sus órbitas son el conjunto $\{0\}$ y, para cada $r \in \mathbf{R}, r > 0$, las circunferencias $\{z \in \mathbf{C} \mid |z| = r\}$.

Ejemplos 8.2.11. *Ejemplo de órbitas y estabilizadores de las acciones de D_4 y S_4 en $\{1,2,3,4\}$ y de $< r_1 >$ y $< r_2 >$ en $\{1,2,3,4\}$.*

Terminamos esta sección usando la idea de órbitas de una acción para demostrar la unicidad de los ciclos que aparecen en la descomposición de una permutación como producto de ciclos disjuntos:

Proposición 8.2.12. *Sea σ un elemento de S_n. Los ciclos que aparecen en la descomposición de σ como producto de ciclos disjuntos están determinados de manera única. Por tanto, la descomposición de σ como producto de ciclos disjuntos salvo por el orden en que escribimos los ciclos.*

Demostración. S_n actúa en $X = \{1, 2, \ldots, n\}$ según vimos en el ejemplo ?? (hay que escribir el ejemplo). Sea $H =< \sigma >$. □

8.3 Orden del estabilizador y cardinal de la órbita

Vemos en esta sección un resultado que relaciona el orden de un grupo finito G, el orden del estabilizador de un elemento x de X y el cardinal de la órbita de x. Para ello necesitamos recordar antes la siguiente definición:

Definición 8.3.1. Sea $f : Z \longrightarrow X$ una aplicación entre dos conjuntos Z y X no vacíos. Dado $x \in X$, la *preimagen* o la *fibra* de x (por f) es el conjunto

$$f^{-1}(x) = \{z \in Z \mid f(z) = x\}.$$

Observación 8.3.2. (1) La fibra de x es no vacía si y solo si x pertenece a la imagen de f.

(2) Existe una biyección entre la imagen de f y el conjunto que tiene por elementos las fibras no vacías de f.

Lema 8.3.3. *Sea*

$$\begin{array}{rccc} \alpha: & G \times X & \longrightarrow & X \\ & (g,x) & \mapsto & gx \end{array}$$

una acción de un grupo G en un conjunto X. Sea $x \in X$. Definimos la aplicación

$$\begin{array}{rccc} \alpha_x: & G & \longrightarrow & X \\ & g & \mapsto & gx. \end{array}$$

Denotamos $H = \mathrm{Stab}(x)$.

(1) La imagen de α_x es la órbita Gx de x.

(2) *Sea $g \in G$. La fibra $\alpha_x^{-1}(gx)$ de gx es $gH = \{gh \mid h \in \mathrm{Stab}(x)\}$; es decir, la fibra de gx es la clase de g respecto de la relación de equivalencia R^H. En particular, existe una biyección entre cualesquiera dos fibras de α_x.*

(3) *Existe una biyección entre el conjunto cociente G/R^H y la órbita Gx.*

Demostración. Que la imagen de α_x es Gx no es sino la definición de órbita.

Sea ahora $gx \in Gx$ y veamos cuál es su fibra por α_x. Tenemos que g' pertenece a la fibra de gx si y solo si $\alpha_x(g') = gx$; es decir, si y solo si $g'x = gx$; es decir, si y solo si $(g^{-1}g')x = g^{-1}(g'x) = g^{-1}(gx) = (g^{-1}g)x = 1x = x$; es decir, si y solo si $g^{-1}g'$ pertenece al estabilizador de x; es decir, si y solo si gR^Hg'; es decir, si y solo si g' pertenece a la clase de equivalencia de g respecto de la relación R^H, que es $gH = \{gh \mid h \in \mathrm{Stab}(x)\}$. Por otra parte, si g_1x y g_2x son dos elementos de Gx, existe una biyección entre sus fibras g_1H y g_2H por la proposición 5.5.5.

Por el apartado (2) los elementos del conjunto cociente G/R^H son las fibras no vacías de α_x. Entonces el apartado (3) se sigue del apartado (1) y de la observación 8.3.2. □

Teorema 8.3.4. *Sea*

$$\begin{array}{rccc} \alpha: & G \times X & \longrightarrow & X \\ & (g,x) & \mapsto & gx \end{array}$$

una acción de un grupo G en un conjunto X. Sea $x \in X$.

(1) *El grupo G es finito si y solo si Gx y $\mathrm{Stab}(x)$ son finitos.*

(2) *Si G es finito entonces*

$$\mathrm{ord}(G) = \mathrm{card}(Gx) \cdot \mathrm{ord}(\mathrm{Stab}(x)), \tag{8.3.4.1}$$

y $\mathrm{card}(Gx) = [G : \mathrm{Stab}(x)]$.

Demostración. Llamamos H al estabilizador de x. Si G es finito, también lo es H y G/R^H y, por el lema 8.3.3 (3), la órbita Gx. Por otra parte, los elementos de G/R^H dan una partición de G. Por el lema 8.3.3 (3) existe una biyección entre Gx y G/R^H y por la proposición 5.5.5, existe una biyección entre un elemento cualquiera gH de G/R^H y H. Entonces si Gx y H son finitos, también lo es G.

El lema 8.3.3 (3) implica que Gx y G/R^H tienen el mismo cardinal. El apartado (2) se sigue entonces del teorema 5.5.9. □

Como aplicación del teorema 8.3.4 damos una demostración de la proposición 5.3.3:

Corolario 8.3.5. (Proposición 5.3.3) *Los isomorfismos afines del plano afín euclídeo estándar $\mathbf{A}^2_{\mathbf{R}}$ que dejan P_n invariante son necesariamente isometrías de $\mathbf{A}^2_{\mathbf{R}}$ y son exactamente las isometrías $id, g, g^2, \ldots, g^{n-1}, r_1, \ldots, r_n$ descritas en la proposición–definición 5.3.2.*

Demostración. En esta demostración usaremos unos mínimos conocimientos de geometría afín, a saber, que un isomorfismo afín trasforma rectas en rectas, que un isomorfismo afín de $\mathbf{A}^2_{\mathbf{R}}$ que deja fijos tres puntos afínmente independientes es la identidad y que giros y reflexiones son isomorfismos afines.

En primer lugar demostramos que el subgrupo G de $\mathrm{Af}(\mathbf{A}^2_{\mathbf{R}})$ formado por aquellos isomorfismos afines de $\mathbf{A}^2_{\mathbf{R}}$ que dejan P_n invariante actúa en el conjunto Σ formado por los vértices de P_n. Sean L y L' dos lados contiguos de P_n que se cortan en un vértice p de P_n. Un elemento φ de G transforma las rectas que contienen a L y L' en dos rectas que contienen otros dos lados de P_n, que tienen que ser necesariamente contiguos pues su intersección es $\varphi(p)$, que, como ha de pertenecer a P_n, debe ser un vértice de P_n. Esto demuestra que G actúa en Σ de la siguiente manera: dado $\varphi \in G$ y $p \in \Sigma$, la acción de φ en p es $\varphi(p)$.

Aplicamos ahora la fórmula 8.3.4.1 a G y a un vértice p_1 de Σ. Recordemos que $o = (0, 0, \ldots, 0)$ es el centro de P_n y que g es el giro de ángulo $2\pi/n$ y centro o. Es claro que $\Sigma = \{p_1, g(p_1), g^2(p_1), \ldots, g^{n-1}(p_1)\}$ por lo que la acción de G en Σ es transitiva. Entonces la fórmula 8.3.4.1 nos dice

$$\mathrm{ord}(G) = n \cdot \mathrm{ord}(\mathrm{Stab}(p_1)). \tag{8.3.5.1}$$

Aplicamos nuevamente la fórmula 8.3.4.1, esta vez al grupo $\mathrm{Stab}(p_1)$ (que al ser subgrupo de G, también actúa en Σ) y a un vértice p_2 contiguo a p_1. Para ello calculamos el cardinal de la órbita de p_2 por la acción de $\mathrm{Stab}(p_1)$ y el orden del estabilizador de p_2 por la acción de $\mathrm{Stab}(p_1)$. Si $\varphi \in \mathrm{Stab}(p_1)$, entonces la recta que contiene a p_1 y p_2 se transforma necesariamente en una recta que contiene a uno de los dos lados que se cortan en p_1. Por otra parte la reflexión con eje la recta por o y p_1 lleva p_2 a un vértice, contiguo a p_1, distinto de p_2. De todo ello deducimos que el cardinal de la órbita de p_2 por la acción de $\mathrm{Stab}(p_1)$ es 2.

Sea ahora H el estabilizador de p_2 por la acción de $\mathrm{Stab}(p_1)$. En ese caso H consiste en aquellos elementos de G que dejan p_1 y p_2 fijos. Sea p_3 el vértice contiguo a p_2 distinto a p_1. Si $\varphi \in H$, como $\varphi(p_2) = p_2$, $\varphi(p_3)$ está en el lado $\overline{p_2p_1}$ o en el lado $\overline{p_2p_3}$. Como $\varphi(p_1) = p_1$, $\varphi(p_3)$ no puede estar en $\overline{p_2p_1}$. Entonces $\varphi(p_3)$ está en $\overline{p_2p_3}$ y $\varphi(p_3) = p_3$. Tenemos pues que φ deja fijos p_1, p_2 y p_3, que son tres puntos afínmente independientes de $\mathbf{A}^2_{\mathbf{R}}$. Por tanto $\varphi = \mathrm{id}$ y el orden de H es 1. Tenemos entonces

$$\mathrm{ord}(\mathrm{Stab}(p_1)) = 2 \cdot 1 = 2. \tag{8.3.5.2}$$

Juntando (8.3.5.1) y (8.3.5.2) vemos que el orden de G es $2n$. Como los elementos de D_n son isomorfismos afines y dejan P_n invariante, D_n es un subgrupo de G. Como D_n tiene también orden $2n$, tenemos que $G = D_n$.

Por último, como los elementos de D_n son giros y reflexiones, que son isometrías de $\mathbf{A}^2_{\mathbf{R}}$, se sigue que los isomorfismos afines que dejan P_n invariante, esto es, los elementos de G, son isometrías. □

Tema 9

Estructura de los grupos abelianos finitamente generados

Hasta ahora hemos visto la estructura de algunos grupos sencillos, como los grupos cíclicos que, o bien son isomorfos a $(\mathbf{Z}, +)$, o bien son isomorfos a $(\mathbf{Z}_n, +)$, para algún $n \in \mathbf{N}$ (corolario 6.3.6) o como los grupos de orden 4, que, o bien son isomorfos a $(\mathbf{Z}_2 \times \mathbf{Z}_2, +)$ o a $(\mathbf{Z}_4, +)$ (ejercicio 1 del tema 6). El propósito de este tema es generalizar estos resultados. Para que esta generalización sea factible nos restringiremos a los grupos abelianos generados por un número finito de elementos. El teorema que obtendremos (teorema 9.2.5) nos permitirá entender de manera transparente la estructura (cuál es del orden de sus elementos, cómo son sus subgrupos...) de los grupos abelianos finitamente generados, de la misma forma que el saber que un grupo cíclico G es isomorfo a $(\mathbf{Z}, +)$ o a $(\mathbf{Z}_n, +)$ nos facilita la comprensión de la estructura de G.

9.1 Generadores y relaciones

En la demostración del corolario 6.3.6 vimos que todo grupo cíclico es un cociente de $(\mathbf{Z}, +)$. En esta sección generalizamos esto a cualquier grupo abeliano finitamente generado (recuerda la proposición-definición 5.4.17). Comenzaremos con un ejemplo de uno de esos grupos. Antes necesitamos la definición de producto de grupos:

Proposición–Definición 9.1.1. Sean $(G_1, \cdot)$ y $(G_2, \cdot)$ dos grupos (no necesariamente abelianos). El producto cartesiano $G_1 \times G_2$ tiene estructura de grupo con respecto a la operación

$$\begin{array}{ccc} (G_1 \times G_2) \times (G_1 \times G_2) & \longrightarrow & (G_1 \times G_2) \\ ((g_1, g_2), (g_1', g_2')) & \mapsto & (g_1 g_1', g_2 g_2'). \end{array}$$

A $G_1 \times G_2$ se le llama *producto* de G_1 y G_2. El producto $G_1 \times G_2$ es abeliano si y solo si G_1 y G_2 son abelianos.

Demostración. La demostración es inmediata y la dejamos como ejercicio. □

Observación 9.1.2. La construcción del producto de dos grupos definida en la proposición-definición 9.1.1 se puede iterar de manera obvia para definir el producto de un número finito de grupos.

Proposición 9.1.3. *Sean $(G_1, \cdot)$ y $(G_2, \cdot)$ dos grupos y sea $G_1 \times G_2$ el grupo producto definido en la definición 9.1.1. Sean H_1 y H_2 dos subgrupos de G_1 y G_2 respectivamente.*

(1) Si $\phi_1 : G_1 \longrightarrow G_1'$ y $\phi_2 : G_2 \longrightarrow G_2'$ son homomorfismos de grupos y $G_1' \times G_2'$ el grupo producto de G_1' y G_2' definido en la definición 9.1.1, entonces la aplicación

$$\begin{array}{rccc} \phi_1 \times \phi_2 : & G_1 \times G_2 & \longrightarrow & G_1' \times G_2' \\ & (g_1, g_2) & \mapsto & (\phi_1(g_1), \phi_2(g_2) \end{array}$$

es un homomorfismo de grupos.

(2) $H_1 \times H_2$ es un subgrupo de $G_1 \times G_2$.

(3) Si H_1 y H_2 son subgrupos normales, entonces $H_1 \times H_2$ es un subgrupo normal de $G_1 \times G_2$.

(4) Si H_1 y H_2 son subgrupos normales, entonces,

$$\frac{G_1 \times G_2}{H_1 \times H_2} \simeq \frac{G_1}{H_1} \times \frac{G_2}{H_2}.$$

Demostración. Las afirmaciones (1), (2), (3) son sencillas a partir de las definiciones grupo, subgrupo, homomorfismo de grupos y grupo producto, por lo que dejamos los detalles como ejercicio. Para demostrar (4), consideramos las proyecciones canónicas $\pi_1 : G_1 \longrightarrow G_1/H_1$ y $\pi_2 : G_2 \longrightarrow G_2/H_2$. El homomorfismo $\pi_1 \times \pi_2$ es sobreyectivo y su núcleo es $H_1 \times H_2$. Entonces el teorema 6.3.3 nos da el isomorfismo $\overline{\pi_1 \times \pi_2}$. □

Ejemplo 9.1.4. Sea $k \in \mathbf{N}$. El producto cartesiano $\mathbf{Z}^k := \mathbf{Z} \times \overset{k)}{\cdots} \times \mathbf{Z}$ es un grupo abeliano con la operación $(n_1, n_2, \ldots, n_k) + (m_1, m_2, \ldots, m_k) := (n_1 + m_1, n_2 + m_2, \ldots, n_k + m_k)$.

Observación 9.1.5. La estructura de grupo de $\mathbf{Z}^k$ se puede obtener de la definición-proposición 9.1.1 y de la observación 9.1.2. Equivalentemente, $(\mathbf{Z}^k, +)$ es el grupo aditivo del anillo producto $(\mathbf{Z}^k, +, \cdot)$.

Notación 9.1.6. En $\mathbf{Z}^k$ usaremos las siguientes notaciones:

(1) $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_k = (0, \ldots, 0, 1)$.

(2) Dado $n \in \mathbf{Z}$ y $v \in \mathbf{Z}^k$, adoptamos la notación:

(i) $nv := v + \overset{n)}{\cdots} + v$, si $n \in \mathbf{N}$;

(ii) $0v := (0, \ldots, 0)$; y

(iii) $nv := (-v) + \overset{-n)}{\cdots} + (-v)$ si $n < 0$.

Dicho de otra forma, en $\mathbf{Z}^k$ usaremos notación *aditiva* en vez de multiplicativa.

Observación 9.1.7. Las propiedades de la suma y el producto en $(\mathbf{Z}, +, \cdot)$ implican para todo $n, n' \in \mathbf{Z}$, $v, v' \in \mathbf{Z}_k$:

(1) $n(v + v') = nv + nv'$;

(2) $(n + n')v = nv + n'v$;

(3) $(nn')v = n(n'v)$.

Observación 9.1.8. En efecto, $\mathbf{Z}^k$ está finitamente generado, puesto que el conjunto $\{e_1, e_2, \ldots, e_k\}$ es un sistema de generadores de $\mathbf{Z}^k$, ya que, si $v = (n_1, n_2, \ldots, n_k)$ es un elemento cualquiera de $\mathbf{Z}^k$, entonces $v = n_1e_1 + n_2e_2 + \cdots + n_ke_k$. De hecho, $\{e_1, e_2, \ldots, e_k\}$ es una *base* de $\mathbf{Z}^k$ en el sentido de que funciona como una base de un espacio vectorial: dado v, la colección ordenada de enteros $(n_1, n_2, \ldots, n_k)$ tal que $v = n_1e_1 + n_2e_2 + \cdots + n_ke_k$ es, obviamente, única[1]. Por analogía con un espacio vectorial, llamaremos a $\{e_1, e_2, \ldots, e_k\}$ base *canónica* de $\mathbf{Z}^k$.

En el corolario 6.3.6 vimos que un grupo G es cíclico si y solo si recibe un homomorfismo sobreyectivo de $(\mathbf{Z}, +)$. Generalizamos a continuación ese resultado.

Lema 9.1.9. *Sea $(G, \cdot)$ un grupo abeliano y sean $g_1, g_2, \ldots, g_k \in G$. Existe un único homomorfismo*

$$\varphi : (\mathbf{Z}^k, +) \longrightarrow (G, \cdot)$$

que cumple $\varphi(e_i) = g_1$.

Demostración. Si existiera φ como en el enunciado, la definición de homomorfismo implicaría que

$$\varphi((n_1, n_2, \ldots, n_k)) = \varphi(n_1e_1 + n_2e_2 + \cdots + n_ke_k) = g_1^{n_1}g_2^{n_2}\cdots g_k^{n_k},$$

por tanto φ sería único. Para comprobar que existe φ como en el enunciado basta ver que la aplicación

$$\begin{array}{rccc} \varphi : & \mathbf{Z}^k & \longrightarrow & G \\ & (n_1, n_2, \ldots, n_k) & \mapsto & g_1^{n_1}g_2^{n_2}\cdots g_k^{n_k} \end{array}$$

es un homomorfismo y que $\varphi(e_i) = g_i$. Lo segundo es inmediato. Lo primero ocurre por ser G abeliano. En efecto, sean $v = (n_1, n_2, \ldots, n_k)$ y $w = (m_1, m_2, \ldots, m_k)$ dos elementos de $\mathbf{Z}^k$. Entonces

$$\varphi(v + w) = \varphi((n_1 + m_1, n_2 + m_2, \ldots, n_k + m_k)) = g_1^{n_1+m_1}g_2^{n_2+m_2}\cdots g_k^{n_k+m_k}.$$

[1] Al grupo $\mathbf{Z}^k$ no se le puede dar estructura de espacio vectorial, pero la notación 9.1.6 nos permite definir una operación externa de $\mathbf{Z}$ sobre $\mathbf{Z}^k$ que, junto con la operación interna de $(\mathbf{Z}^k, +)$, dota a $\mathbf{Z}^k$ de lo que se denomina estructura de $\mathbf{Z}$-*módulo*, que es una generalización de la noción de espacio vectorial. Las propiedades que ha de cumplir la operación externa de un módulo son las tres que aparecen en la observación 9.1.7 y otra más, $1v = v$, que se cumple de manera obvia. Estas propiedades son las mismas que las de la definición de espacio vectorial; si $\mathbf{Z}^k$ no es un espacio vectorial es porque $\mathbf{Z}$ no es un cuerpo. No solo $\mathbf{Z}^k$ posee estructura de $\mathbf{Z}$–módulo, todo grupo abeliano también la tiene.

Por otra parte, al ser G abeliano,

$$g_1^{n_1+m_1} g_2^{n_2+m_2} \cdots g_k^{n_k+m_k} = (g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k})(g_1^{m_1} g_2^{m_2} \cdots g_k^{m_k}) = \varphi(v)\varphi(w).$$

□

Proposición 9.1.10. *Un grupo $(G, \cdot)$ es abeliano y está finitamente generado por los elementos $g_1, g_2, \ldots, g_k$ si y solo si existe un homomorfismo de grupos sobreyectivo*

$$\varphi : (\mathbf{Z}^k, +) \longrightarrow (G, \cdot)$$

que cumple $\varphi(e_i) = g_i$.

Demostración. Si existe φ como en el enunciado, según la demostración del lema 9.1.9

$$\varphi((n_1, n_2, \ldots, n_k)) = g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k}.$$

Por tanto, si φ es sobreyectivo, entonces todos los elementos de G están en la imagen de φ, por lo que son productos finitos de elementos de $\{g_1, g_2, \ldots, g_k\}$. Por ello G está generado por los elementos $g_1, g_2, \ldots, g_k$. Por el teorema de isomorfía, G es un cociente de $\mathbf{Z}^k$. Como $\mathbf{Z}^k$ es abeliano, G es abeliano.

Supongamos ahora que G es abeliano y está finitamente generado por los elementos $g_1, g_2, \ldots, g_k$. Según el lema existe un único homomorfismo φ de $\mathbf{Z}^k$ a G tal que $\varphi(e_i) = g_i$. Como G es abeliano y $G = <g_1, g_2, \ldots, g_k>$, todo elemento de G es de la forma $g_1^{m_1} g_2^{m_2} \cdots g_k^{m_k}$ para ciertos $n_1, n_2, \ldots, n_k \in \mathbf{Z}$, por lo que $\varphi(n_1 e_1 + n_2 e_2 + \cdots + n_k e_k) = g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k}$. Esto prueba que φ es sobreyectivo. □

Definición 9.1.11. Sea $(G, \cdot)$ un grupo abeliano generado por los elementos $g_1, g_2, \ldots, g_k$. Diremos que el homomorfismo φ de la proposición 9.1.10 es una *presentación* de G. A los elementos no nulos del núcleo de φ los llamaremos *relaciones* de $g_1, g_2, \ldots, g_k$.

Proposición 9.1.12. *Para todo $k \in \mathbf{N}$, todo subgrupo de $\mathbf{Z}^k$ está finitamente generado.*

Demostración. Hacemos la demostración por inducción sobre k. Si $k = 1$, entonces, según el ejercicio 7 del tema 5, todos los subgrupos de $\mathbf{Z}$ son cíclicos y, en particular, finitamente generados. Consideramos las aplicaciones

$$\begin{array}{rccc} \pi' : & \mathbf{Z}^k & \longrightarrow & \mathbf{Z}^{k-1} \\ & (x_1, \ldots, x_{k-1}, x_k) & \mapsto & (x_1, \ldots, x_{k-1}) \end{array}$$

y

$$\begin{array}{rccc} \pi'' : & \mathbf{Z}^k & \longrightarrow & \mathbf{Z} \\ & (x_1, \ldots, x_{k-1}, x_k) & \mapsto & x_k\,. \end{array}$$

Es inmediato comprobar que π' y π'' son homomorfismos de grupos. Sea H un subgrupo de $\mathbf{Z}^k$. Entonces $H' = \pi'(H)$ es un subgrupo de $\mathbf{Z}^{k-1}$ y $H'' = \pi''(H)$ es un subgrupo de $\mathbf{Z}$. Por la hipótesis de inducción y por el resultado para $k = 1$, H' y H'' están finitamente generados. Sea $\{h'_1, \ldots, h'_s\}$ un sistema de generadores de H' y sea $\{h''_1, \ldots, h''_t\}$ un sistema de generadores de H''. Entonces $\{(h'_1, 0), \ldots, (h'_s, 0), (0, \ldots, 0, h''_1), \ldots, (0, \ldots, 0, h''_t)\}$ es un sistema de generadores de H, por lo que H está finitamente generado. □

Observación 9.1.13. Se sigue del teorema 6.3.3 y de la proposición 9.1.10 que un grupo $(G,\cdot)$ es abeliano y está finitamente generado si y solo si $(G,\cdot)$ es isomorfo a un cociente de $(\mathbf{Z}^k,+)$ para algún $k \in \mathbf{N}$. Concretamente $(G,\cdot)$ es isomorfo al cociente de $(\mathbf{Z}^k,+)$ por el núcleo de la presentación φ de la proposición 9.1.10. La proposición 9.1.12 nos dice que el núcleo de φ está generado por una cantidad finita de relaciones. Se dice entonces que $(G,\cdot)$ no solamente está finitamente generado sino también *finitamente presentado*. Como $(G,\cdot)$ está determinado salvo isomorfismo por el cociente de $(\mathbf{Z}^k,+)$ por el núcleo de φ, el grupo abeliano finitamente generado $(G,\cdot)$ está determinado (no de forma única, ya que $(G,\cdot)$ posee sistemas de generadores con distintos cardinales) por el número k y por un conjunto finito de relaciones. Como cada una de esas relaciones es una combinación entera de $e_1,\ldots,e_k$, el grupo abeliano finitamente generado $(G,\cdot)$ está determinado por una colección finita de números enteros.

9.2 El teorema de estructura

Como apuntamos al comienzo de este tema, nuestra intención es dar un teorema (teorema 9.2.5) que nos permita entender la estructura para los grupos abelianos finitamente generados. Por ello, en lo que queda de tema y a no ser que se diga explícitamente otra cosa, un grupo será un grupo abeliano finitamente generado. La observación 9.1.13 nos decía que un grupo abeliano finitamente generado está determinado por una colección finita de números enteros. Comenzamos "codificando" esta información en forma de matríz:

Definición 9.2.1. Sea

$$\varphi : (\mathbf{Z}^k,+) \longrightarrow (G,\cdot)$$

una presentación de un grupo $(G,\cdot)$ y sea $\mathrm{Ker}\varphi = <r_1, r_2, \ldots, r_s>$, donde $r_i = a_{i1}e_1 + \cdots + a_{ik}e_k$, para todo $i = 1,\ldots,s$. Asociamos a $r_1, r_2, \ldots, r_s$ la matriz $s \times k$ de elementos enteros

$$M = \begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{s1} & \cdots & a_{sk} \end{pmatrix}.$$

Observación 9.2.2. Dada una presentación φ como en la definición 9.2.1, como $\mathrm{Ker}\varphi$ está generado por $r_1,\ldots,r_s$, por la proposición 9.1.10 existe un homomorfismo

$$\psi' : \mathbf{Z}^s \longrightarrow \mathrm{Ker}\varphi$$

que cumple $\psi'(u_i) = r_i$, donde $u_1 = (1,0,\ldots,0),\ldots,u_s = (0,\ldots,0,1) \in \mathbf{Z}^s$. Componiendo ψ' con la inclusión de $\mathrm{Ker}\varphi$ en $\mathbf{Z}^k$ obtenemos un homomorfismo

$$\psi : \mathbf{Z}^s \longrightarrow \mathbf{Z}^k.$$

Si definimos la matriz de ψ respecto de las bases canónicas (véase la observación 9.1.8) de $\mathbf{Z}^s$ y $\mathbf{Z}^k$ por columnas, como se acostumbra a hacer para aplicaciones lineales entre espacios vectoriales, dicha matriz no es sino la traspuesta de la matriz asociada a

$r_1, r_2, \ldots, r_s$. Por tanto, dar la matriz asociada a un sistema de generadores del núcleo de una presentación φ de un grupo (abeliano finitamente generado) G es equivalente a dar un homomorfismo de grupos ψ entre $\mathbf{Z}^s$ y $\mathbf{Z}^k$. Recuperamos el grupo G como

$$\frac{\mathbf{Z}^k}{\mathrm{im}\psi} \simeq \frac{\mathbf{Z}^k}{\mathrm{Ker}\varphi} \simeq G.$$

Ejemplo 9.2.3. Sea G un grupo (abeliano) generado por cuatro elementos g_1, g_2, g_3 y g_4. Sea $\{e_1, e_2, e_3, e_4\}$ la base canónica de $\mathbf{Z}^4$. Sea

$$\varphi : \mathbf{Z}^4 \longrightarrow G$$

la presentación que cumple $\varphi(e_i) = g_i$ y sea

$$\mathrm{Ker}\varphi = <r_1 = 12e_2 + 40e_4, r_2 = 6e_1 + 28e_2 + 60e_4, r_3 = 60e_1 + 20e_2 + 40e_3> .$$

Entonces

$$G \simeq \frac{\mathbf{Z}^4}{<r_1, r_2, r_3>}$$

y la matriz asociada a r_1, r_2, r_3 es

$$M = \begin{pmatrix} 0 & 12 & 0 & 40 \\ 6 & 28 & 0 & 60 \\ 60 & 20 & 40 & 0 \end{pmatrix}.$$

El número de generadores del grupo G del ejemplo 9.2.3 y las relaciones r_1, r_2, r_3 o, de manera equivalente, la matriz M, determinan G salvo isomorfismo, pero nos dicen poco sobre cómo es G. Por ejemplo, no sabemos a primera vista si G es finito o infinito, cuántos elementos de orden finito tiene G o cuáles son los órdenes de esos elementos. Sería deseable tener una presentación para G y una matriz asociada que nos permitiera responder de forma rápida y fácil a algunas de esas preguntas. En el siguiente ejemplo la estructura de G está más clara:

Proposición 9.2.4. *Sea G un grupo (abeliano) generado por k elementos $g_1, \ldots, g_k$. Sea $\{e_1, \ldots, e_k\}$ la base canónica de $\mathbf{Z}^k$. Sea*

$$\varphi : \mathbf{Z}^k \longrightarrow G$$

la presentación que cumple $\varphi(e_i) = g_i$, sea $0 \leq s \leq k$, sean $m_1, \ldots, m_s \in \mathbf{N}$ y sea

$$\mathrm{Ker}\varphi = <r_1 = m_1e_1, \ldots, r_s = m_se_s> .$$

Entonces la matriz asociada a $r_1, r_2, \ldots, r_s$ es la matriz

$$\begin{pmatrix} m_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & m_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots & & \vdots \\ 0 & 0 & \cdots & m_s & 0 & \cdots & 0 \end{pmatrix} \tag{9.2.4.1}$$

(cuyas únicas entradas no nulas son $m_1, \ldots, m_s$), y

$$G \simeq \frac{\mathbf{Z}^k}{<r_1, \ldots, r_s>} \simeq \mathbf{Z}_{m_1} \times \cdots \mathbf{Z}_{m_s} \times \mathbf{Z}^{r-s} \tag{9.2.4.2}$$

(como no hemos excluido la posibilidad de que alguno de los m_i sea 1, $\mathbf{Z}_{m_i}$ sería en ese caso un grupo formado por un solo elemento, es decir, isomorfo al grupo nulo; como tampoco excluimos la posibilidad $s = k$, adoptamos el convenio de que en ese caso no aparece ningún factor isomofo a $\mathbf{Z}$ en (9.2.4.2)*).*

Demostración. Recordemos primero que, según vimos en la demostración del corolario 6.3.6, para todo $n \in \mathbf{N}$, el grupo aditivo $(\mathbf{Z}_n, +)$ del anillo $(\mathbf{Z}_n, +, \cdot)$, el grupo aditivo $(\mathbf{Z}/(n), +)$ del anillo $(\mathbf{Z}/(n), +, \cdot)$ y el grupo cociente $\mathbf{Z}/<n>$ de $(\mathbf{Z}, +)$ son los tres isomorfos. Entonces los grupos $\mathbf{Z}_{m_1} \times \cdots \mathbf{Z}_{m_s} \times \mathbf{Z}^{k-s}$ y $\frac{\mathbf{Z}}{<m_1>} \times \cdots \times \frac{\mathbf{Z}}{<m_s>} \times \mathbf{Z}^{k-s}$ son isomorfos y trabajaremos con el segundo de ellos. Por otra parte tenemos que

$$< r_1, \ldots, r_s > = < m_1 > \times \cdots \times < m_s > \times < 0 > \times \cdots \times < 0 >,$$

de donde $\frac{\mathbf{Z}^k}{<r_1, \ldots, r_s>}$ es isomorfo a $\frac{\mathbf{Z}}{<m_1>} \times \cdots \times \frac{\mathbf{Z}}{<m_s>} \times \mathbf{Z}^{k-s}$ por la proposición 9.1.3. □

La estructura de un grupo G con una presentación y una matriz como la de (9.2.4.1) es más transparente que la estructura del grupo del ejemplo 9.2.3. Por ejemplo, si G es como en la proposición 9.2.4 sabemos que G es infinito si y solo si $s < k$. También conocemos cuántos elementos de orden finito tiene G (concretamente, $m_1 \cdots m_s$). Por tanto, dado un grupo (abeliano finitamente generado) G queremos una presentación para G y una matriz asociada M que sea como (9.2.4.1) e incluso le pediremos a las entradas de M una condición adicional (que los elementos no nulos de M sean mayores que 1 y que un elemento no nulo divida a los elementos no nulos de las filas siguentes a las suya). Veremos que siempre podremos conseguir una matriz así para G y como resultado obtendremos el siguiente teorema:

Teorema 9.2.5. *(de estructura de los grupos abelianos finitamente generados; factores invariantes). Sea G un grupo abeliano finitamente generado. Existen r, s números enteros no negativos y, si $s > 0$, números naturales $d_1, d_2, \ldots, d_s$ tales que $d_1 > 1$,*

$$d_1 \text{ divide a } d_2, d_2 \text{ divide a } d_3, \ldots, d_{s-1} \text{ divide a } d_s \tag{9.2.5.1}$$

y G es isomorfo

$$(\mathbf{Z}_{d_1} \times \mathbf{Z}_{d_2} \times \cdots \times \mathbf{Z}_{d_s} \times \mathbf{Z}^r, +). \tag{9.2.5.2}$$

Los números $r, s, d_1, d_2, \ldots, d_s$ están determinados por G de forma única, es decir, si r', s' son números enteros no negativos y ${d_1}', {d_2}', \ldots, {d_{s'}}'$ son números naturales tales que ${d_1}' > 1$, ${d_1}'$ divide a ${d_2}'$, ${d_2}'$ divide a ${d_3}', \ldots, {d_{s-1}}'$ divide ${d_s}'$ y G es isomorfo tanto a

$$(\mathbf{Z}_{d_1} \times \mathbf{Z}_{d_2} \times \cdots \times \mathbf{Z}_{d_s} \times \mathbf{Z}^r, +).$$

como a

$$(\mathbf{Z}_{d_1'} \times \mathbf{Z}_{d_2'} \times \cdots \times \mathbf{Z}_{d_{s'}'} \times \mathbf{Z}^{r'}, +),$$

entonces $r = r'$, $s = s'$ *y* $d_1 = d_1'$, $d_2 = d_2' \ldots$, $d_s = d_{s'}'$.

Definición 9.2.6. Sea G como en el teorema 9.2.5.

(1) A los números naturales $d_1, d_2, \ldots, d_s$ de (9.2.5.2) se les denomina *coeficientes de torsión* o *factores invariantes* de G.

(2) Al número entero no negativo r de (9.2.5.2) se le llama *rango* de G.

(3) Si $r \in \mathbf{N}$ y G es isomorfo a $(\mathbf{Z}^r, +)$ decimos que G es un grupo *libre de rango* r.

Dado un grupo abeliano G finitamente generado, a partir de su descomposición en factores invariantes ((9.2.5.2)) podemos obtener otra descomposición, llamada *descomposición primaria*, que también es única para G:

Teorema 9.2.7. *(de estructura de los grupos abelianos finitamente generados; descomposición primaria). Sea G un grupo abeliano finitamente generado. Existen r, t números enteros no negativos y, si $t > 0$, números naturales $q_1, q_2, \ldots, q_t$ que son potencias (positivas) de números primos, no necesariamente distintos tales que G es isomorfo*

$$(\mathbf{Z}_{q_1} \times \mathbf{Z}_{q_2} \times \cdots \times \mathbf{Z}_{q_t} \times \mathbf{Z}^r, +). \tag{9.2.7.1}$$

Los números $r, t, q_1, q_2, \ldots, q_s$ están determinados por G, es decir, son únicos. En particular, si r', t' son números enteros no negativos y $q_1', q_2', \ldots, q_{t'}'$ son potencias (positivas) de números primos y

$$(\mathbf{Z}_{q_1} \times \mathbf{Z}_{q_2} \times \cdots \times \mathbf{Z}_{q_t} \times \mathbf{Z}^r, +). \tag{9.2.7.2}$$

es isomorfo a

$$(\mathbf{Z}_{q_1'} \times \mathbf{Z}_{q_2'} \times \cdots \times \mathbf{Z}_{q_{t'}'} \times \mathbf{Z}^{r'}, +), \tag{9.2.7.3}$$

entonces $r = r'$, $t = t'$ y, si ordenamos los $q_1, \ldots, q_t$ de forma que

(i) si el primo que divide a q_i es menor que el primo que divide a q_j, entonces $i < j$, y

(ii) cuando q_i y q_j son potencias del mismo primo, si $q_i < q_j$, entonces $i < j$,

y hacemos lo mismo para los $q_1', \ldots, q_t'$, entonces $q_1 = q_1'$, $q_2 = q_2' \ldots$, $q_t = q_t'$.

Observación 9.2.8. (1) Si $r = 0$ se entiende que el último factor de (9.2.5.2) y (9.2.7.1) no aparece.

(2) Si $s = 0$ se entiende que solo el último factor de (9.2.5.2) y (9.2.7.1) aparece.

(3) Si $r = s = 0$ se entiende que el grupo de (9.2.5.2) y (9.2.7.1) es el grupo trivial, isomorfo a <0>.

Dado un grupo abeliano finitamente generado G, la existencia de una descomposición como (9.2.5.2) se puede demostrar de varias formas. Nosotros veremos una demostración constructiva. La idea es pasar de la matriz M asociada a las relaciones de una presentación cualquiera de G (que siempre existe una presentación y una matriz para G se deduce de las proposiciones 9.1.10 y 9.1.12) a otra matriz M' y otra presentación de G, tal que M' sea como en (9.2.4.1) e, incluso, tal que las entradas no nulas de M' satisfagan lo que se pide en (9.2.5.2). La manera de pasar de M a otra matriz M' más adecuada es realizando *operaciones elementales*. Definimos estas operaciones a continuación y vemos qué consecuencias tienen:

Definición 9.2.9. Sea

$$M = \begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{l1} & \cdots & a_{lk} \end{pmatrix}$$

una matriz con elementos en $\mathbf{Z}$. Llamamos *operación elemental* en las filas de M a una operación de uno de estos tres tipos:

(i) intercambio de dos filas;

(ii) sustitución de una fila F por $F + nF'$, donde $n \in \mathbf{Z}$ y F' es otra fila de M;

(iii) multiplicación de una fila de M por una unidad de $\mathbf{Z}$, es decir, por 1 o -1.

De manera análoga, llamamos *operación elemental* en las columnas de M a una operación de uno de estos tres tipos:

(i') intercambio de dos columnas;

(ii') sustitución de una columna C por $C + nC'$, donde $n \in \mathbf{Z}$ y C' es otra columna de M;

(iii') multiplicación de una columna de M por una unidad de $\mathbf{Z}$, es decir, por 1 o -1.

Proposición 9.2.10. *Sea G un grupo abeliano finitamente generado, sea*

$$\varphi : \mathbf{Z}^k \longrightarrow G$$

una presentación, sean $r_1, \ldots, r_s$ generadores del núcleo de φ y sea M la matriz asociada a $r_1, \ldots, r_s$.

(1) Si M' es la matriz que se obtiene al realizar una operación elemental en las filas de M, entonces M' es la matriz asociada a otro sistema de generadores del núcleo de φ.

(2) Si M' es la matriz que se obtiene al realizar una operación elemental en las columnas de M, entonces M' es la matriz asociada a un sistema de generadores del núcleo de otra presentación φ' de G.

Demostración. Sea M' la matriz que se obtiene al realizar una operación elemental en las filas de M. Si la operación elemental es como (i) de la definición 9.2.9, entonces M' es la matriz asociada a las relaciones $r_1, \ldots, r_s$ donde simplemente hemos intercambiado en la lista la posición de dos de ellas.

Si la operación elemental es como (iii) de la definición 9.2.9, por ejemplo, si multiplicamos la fila i-ésima por -1, entonces M' es la matriz asociada a $r_1, \ldots, r_{i-1}, -r_i, r_{i+1}, \ldots, r_s$, que es también un sistema de generadores del núcleo de φ.

Finalmente, si la operación elemental es como (ii) de la definición 9.2.9, por ejemplo, si cambiamos la fila i-ésima F_i por la combinación $F_i + aF_j$ ($a \in \mathbf{Z}$) de la fila i-ésima F_i y fila j-ésima F_j, entonces M' es la matriz asociada a $r'_1 = r_1, \ldots, r'_{i-1} = r_{i-1}, r'_i = r_i + ar_j, r'_{i+1} = r_{i+1}, \ldots, r'_s = r_s$, que también es un sistema de generadores del núcleo de φ. En efecto, se tiene $r_1 = r'_1, \ldots, r_{i-1} = r'_{i-1}, r_i = r'_i - ar'_j, r_{i+1} = r'_{i+1}, \ldots, r_s = r'_s$, por lo que una combinación entera de $r_1, \ldots, r_s$ es también una combinación entera de $r'_1, \ldots, r'_s$.

Sea ahora M' la matriz que se obtiene al realizar una operación elemental en las columnas de M. Para cada i, sea $g_i = \varphi(e_i)$. Si la operación elemental es como (i') de la definición 9.2.9, por ejemplo, si intercambiamos la columna i-ésima y la j-ésima, consideramos la presentación

$$\varphi' : \mathbf{Z}^k \longrightarrow G$$

que cumple $\varphi'(e_l) = g_l$ si $l \neq i, j$, $\varphi'(e_i) = g_j$ y $\varphi'(e_j) = g_i$. Entonces M' es la matriz asociada a un sistema de generadores del núcleo de φ'; estos generadores se obtienen intercambiando e_i y e_j en $r_1, r_2, \ldots, r_s$.

Sea ahora una operación elemental es como (ii') de la definición 9.2.9, por ejemplo, cambiemos la columna i-ésima C_i por la combinación $C_i + aC_j$ ($a \in \mathbf{Z}$) de la columna i-ésima C_i y la columna j-ésima C_j. Según el lema 9.1.9 existe un homomorfismo

$$\psi : \mathbf{Z}^k \longrightarrow \mathbf{Z}^k$$

que cumple $\psi(e_l) = e_l$ si $l \neq j$ y $\psi(e_j) = e_j - ae_i$. De nuevo por el lema 9.1.9 existe un homomorfismo

$$\psi' : \mathbf{Z}^k \longrightarrow \mathbf{Z}^k$$

que cumple $\psi'(e_l) = e_l$ si $l \neq j$ y $\psi'(e_j) = e_j + ae_i$. Es claro que ψ y ψ' son inversos uno del otro, por lo que ψ es un isomorfismo. Definamos $\varphi' := \varphi \circ \psi$. Como φ es sobreyectivo y ψ es un isomorfismo, φ' también es sobreyectivo, es decir,

$$\varphi' : \mathbf{Z}^k \longrightarrow G$$

es una presentación de G (concretamente, φ' es el homomorfismo que cumple $\varphi'(e_l) = g_l$ si $l \neq j$ y $\varphi'(e_j) = g_i^{-a} g_j$). Para todo l, sea $r'_l = \psi'(r_l)$. El núcleo de φ' es

$$\mathrm{Ker}\varphi' = \varphi'^{-1}(1_G) = \psi^{-1}(\varphi^{-1}(1_G)) = \psi^{-1}(\mathrm{Ker}\varphi) = \psi'(\mathrm{Ker}\varphi) = \psi'(<r_1, \ldots, r_s>) = <r'_1, \ldots, r'_s>,$$

es decir, el núcleo de φ' está generado por $r'_1, \ldots, r'_s$. Por otra parte, se comprueba fácilmente que M' es la matriz asociada a $r'_1, \ldots, r'_s$.

Por último, si la operación elemental es como (iii') de la definición 9.2.9, por ejemplo, si multiplicamos la columna i-ésima por -1, consideramos la presentación

$$\varphi' : \mathbf{Z}^k \longrightarrow G$$

que cumple $\varphi'(e_l) = g_l$ si $l \neq i$ y $\varphi'(e_i) = g_j^{-1}$. Si $r_h = a_{h,1}e_1 + \cdots + a_{h,k}e_k$, sea

$$r'_h = a_{h,1}e_1 + \cdots + a_{h,i-1}e_{i-1} - a_{h,i}e_i + a_{h,i+1}e_{i+1} + \cdots + a_{h,k}e_k.$$

Razonando como en el párrafo anterior concluimos que $r'_1, \ldots, r'_s$ generan el núcleo de φ'. Por otra parte, es claro que M' es la matriz asociada a $r'_1, \ldots, r'_s$. □

Antes de dar la demostración del teorema 9.2.5, vemos cómo hallar una descomposición como la de (9.2.5.2) en algunos ejemplos:

Ejemplo 9.2.11. Sea G, φ y M como en el ejemplo 9.2.3. Queremos realizar operaciones elementales en M para obtener una matriz como (9.2.4.1). Para conseguir que la primera entrada de M sea no nula intercambiamos la primera y segunda fila:

$$M = \begin{pmatrix} 0 & 12 & 0 & 40 \\ 6 & 28 & 0 & 60 \\ 60 & 20 & 40 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 6 & 28 & 0 & 60 \\ 0 & 12 & 0 & 40 \\ 60 & 20 & 40 & 0 \end{pmatrix} = M_1.$$

Queremos ahora hacer ceros en la primera fila de M_1. Primero hacemos un cero en la última entrada de la primera fila; para ello realizamos la operación elemental $C_4 \to C_4 - 10C_1$:

$$M_1 = \begin{pmatrix} 6 & 28 & 0 & 60 \\ 0 & 12 & 0 & 40 \\ 60 & 20 & 40 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 6 & 28 & 0 & 0 \\ 0 & 12 & 0 & 40 \\ 60 & 20 & 40 & -600 \end{pmatrix} = M_2.$$

Ahora queremos hacer un cero en la segunda entrada de la primera fila de M_2. Como 6 no divide a 28, no podemos conseguirlo con una sola operación elemental. En lugar de ellos hacemos varias, concretamente

$$C_2 \to C_2 - 4C_1, C_1 \to C_1 - C_2, C_2 \to C_2 - 2C_1,$$

transformando así la matriz M_2:

$$M_2 = \begin{pmatrix} 6 & 28 & 0 & 0 \\ 0 & 12 & 0 & 40 \\ 60 & 20 & 40 & -600 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 6 & 4 & 0 & 0 \\ 0 & 12 & 0 & 40 \\ 60 & -220 & 40 & -600 \end{pmatrix} \rightsquigarrow$$

$$\begin{pmatrix} 2 & 4 & 0 & 0 \\ -12 & 12 & 0 & 40 \\ 280 & -220 & 40 & -600 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 & 0 \\ -12 & 36 & 0 & 40 \\ 280 & -780 & 40 & -600 \end{pmatrix} = M_3$$

(las dos primeras operaciones corresponden a los pasos del algoritmo de Euclídes para calcular el máximo común divisor de 6 y 28, que es 2; por eso, al realizarlas, obtenemos

que la primera entrada de la primera fila sí divide a la segunda entrada). Finalmente hacemos ceros en la primera columna de M_3, realizando las operaciones elementales

$$F_2 \to F_2 + 6F_1, F_3 \to F_3 - 140F_1$$

que transforman así la matriz M_3:

$$M_3 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ -12 & 36 & 0 & 40 \\ 280 & -780 & 40 & -600 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 36 & 0 & 40 \\ 280 & -780 & 40 & -600 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 36 & 0 & 40 \\ 0 & -780 & 40 & -600 \end{pmatrix} = M_4.$$

Llegar a partir de M_4 a una matriz como (9.2.4.1) es un problema más sencillo, ya que es suficiente considerar operaciones elementales en la submatriz

$$\begin{pmatrix} 36 & 0 & 40 \\ -780 & 40 & -600 \end{pmatrix}$$

de M_4, que equivale a hacer operaciones en las dos últimas filas y las tres últimas columnas de M'. Así continuamos realizando las operaciones elementales

$$C_4 \to C_4 - C_2, C_2 \leftrightarrow C_4, C_4 \to C_4 - 9C_2, F_3 \to F_3 - 45F_2, C_4 \to C_4 + 60C_3$$

a M_4, transformándola así:

$$M_4 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 36 & 0 & 40 \\ 0 & -780 & 40 & -600 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 36 & 0 & 4 \\ 0 & -780 & 40 & 180 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 36 \\ 0 & 180 & 40 & -780 \end{pmatrix} \rightsquigarrow$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 180 & 40 & -2400 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 40 & -2400 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 40 & 0 \end{pmatrix} = M_5.$$

La proposición 9.2.10 nos asegura que la matriz M_5 es la matriz asociada a un sistema de generadores del núcleo de cierta presentación de G, por lo que

$$G \simeq \frac{\mathbf{Z}^4}{<2e_1, 4e_2, 40e_3>}.$$

La proposición 9.2.4 nos dice que

$$G \simeq (\mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_{40} \times \mathbf{Z}, +),$$

por lo que el rango de G es 1 y sus coeficientes de torsión son 2, 4 y 40.

En el ejemplo 9.2.11 haciendo operaciones elementales en M obtuvimos una matriz, M_5, como (9.2.4.1), tal que sus elementos en la diagonal cumplían los requisitos (9.2.5.1) de los coeficientes de torsión. En el siguiente ejemplo vemos qué hacer si tenemos una matriz como (9.2.4.1) cuyos elementos en la diagonal no cumplen (9.2.5.1):

Ejemplo 9.2.12. Sea G un grupo abeliano finitamente generado, sea

$$\varphi : \mathbf{Z}^2 \longrightarrow G$$

una presentación de G y sea

$$M = \begin{pmatrix} 6 & 0 \\ 0 & 28 \end{pmatrix}$$

una matriz asociada a un sistema de generadores del núcleo de φ. En el ejemplo 9.2.11 vimos cómo abordar la situación en la que un elemento no dividía a todos los elementos de su fila o columna. Lo primero que hacemos es una operación elemental, $F_1 \to F_1 + F_2$, para ponernos en esa situación. Así la matriz M se transforma en

$$M' = \begin{pmatrix} 6 & 28 \\ 0 & 28 \end{pmatrix}.$$

Hacemos las operaciones

$$C_2 \to C_2 - 4C_1, C_1 \to C_1 - C_2, C_2 \to C_2 - 2C_1, F_2 \to F_2 + 14F_1$$

en M' y M' se transforma en

$$M'' = \begin{pmatrix} 2 & 0 \\ 0 & 84 \end{pmatrix}.$$

Por las proposiciones 9.2.4 y 9.2.10,

$$G \sim (\mathbf{Z}_2 \times \mathbf{Z}_{84}, +).$$

En este caso G tiene rango 0 y sus coeficientes de torsión son 2 y 84.

Vemos una forma alternativa de proceder. Que

$$M = \begin{pmatrix} 6 & 0 \\ 0 & 28 \end{pmatrix}$$

implica, por la proposición 9.2.4, que

$$G \sim (\mathbf{Z}_6 \times \mathbf{Z}_{28}, +).$$

El corolario 3.4.10 nos dice que el anillo $(\mathbf{Z}_6 \times \mathbf{Z}_{28}, +, \cdot)$ es isomorfo al anillo $(\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_4 \times \mathbf{Z}_7, +, \cdot)$ y el corolario 3.4.11 nos dice que este lo es, a su vez, al anillo $(\mathbf{Z}_2 \times \mathbf{Z}_{84}, +, \cdot)$. Entonces el grupo $(\mathbf{Z}_6 \times \mathbf{Z}_{28}, +)$ es isomorfo al grupo $(\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_4 \times \mathbf{Z}_7, +)$ y este a su vez al grupo $(\mathbf{Z}_2 \times \mathbf{Z}_{84}, +,)$.

Dado un grupo abeliano finitamente generado G, los argumentos, elementales, que aparecen en los ejemplos 9.2.11 y 9.2.12 nos sirven para dar una demostración constructiva de la existencia de la descomposición en (9.2.5.2) (de hecho, es posible dar un algoritmo para obtener esa descomposición). En dichos ejemplos podemos vislumbrar dos argumentos inductivos, uno sobre el tamaño de la matriz y otro sobre el valor absoluto de las entradas de la matriz. A continuación hacemos esta idea precisa.

Proposición 9.2.13. *Sea M una matriz con entradas enteras. Usando operaciones elementales como las de la definición 9.2.9, se puede obtener una matriz con entradas no negativas*

$$M' = \begin{pmatrix} m_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & m_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots & & \vdots \\ 0 & 0 & \cdots & m_s & 0 & \cdots & 0 \end{pmatrix}, \tag{9.2.13.1}$$

tal que, para algún $0 \leq s' \leq s$, entonces $m_{s'+1} = \cdots = m_s = 0$, $m_1, m_2, \ldots, m_{s'} \neq 0$ y m_1 divide a m_2, m_2 divide a $m_3, \ldots, m_{s'-1}$ divide a $m_{s'}$.

Demostración. Si M es la matriz nula, no hay nada que demostrar, ya que podemos tomar $M' = M$ y $s' = 0$. Supongamos pues que M es no nula. Haremos la demostración realizando una doble inducción, inducción completa sobre el número de elementos de M por una parte e inducción completa sobre el mínimo del valor absoluto de los elementos de M por otra. El paso inicial de la inducción sobre el número de elementos es trivial ya que en ese caso M es 1×1 y tomando $M' = M$, M' cumple todos los requisitos pedidos.

Veamos ahora el paso inicial para la inducción sobre el mínimo del valor absoluto de los elementos de M. En ese caso, existe un elemento de M que es 1 o -1. Demostramos que M cumple la proposición haciendo inducción completa sobre el número de elementos de M. Sea s el número de filas y sea k el número de columnas de M. Realizando operaciones elementales del tipo (i) y (i'), obtenemos una matriz cuyo primer elemento es 1 o -1. Realizando si es necesario una operación elemental del tipo (iii) o (iii') obtenemos una matriz cuyo primer elemento es 1. Si $k = 1$ o $s = 1$, haciendo operaciones elementales del tipo (ii) o (ii') obtenemos una matriz cuyos elementos son todos nulos menos el primero, que es 1. Esta matriz cumple los requisitos pedidos a M'. Si $k, s > 1$, haciendo operaciones elementales de tipo (ii) y (ii') obtenemos una matriz

$$\widehat{M} = \begin{pmatrix} 1 & 0 \\ 0 & \widetilde{M} \end{pmatrix},$$

donde 0 representa $k-1$ entradas nulas en la primera fila y $s-1$ entradas nulas en la primera columna y $\widetilde{M}$ es una matriz $(s-1) \times (k-1)$. Si $\widetilde{M}$ es la matriz nula, entonces $\widehat{M}$ cumple los requisitos pedidos a M' y ya hemos terminado. Si $\widetilde{M}$ no es la matriz nula, como tiene menos elementos que M, podemos aplicar la hipótesis de inducción. Así pues, realizando operaciones elementales en $\widetilde{M}$, obtenemos una matriz $\widetilde{M'}$ que cumple los requisitos pedidos a M'. Entonces la matriz

$$\widehat{M'} = \begin{pmatrix} 1 & 0 \\ 0 & \widetilde{M'} \end{pmatrix},$$

se obtiene realizando operaciones elementales en $\widehat{M}$ y como 1 divide la primera entrada de $\widetilde{M'}$, la matriz $\widehat{M'}$ cumple los requisitos pedidos a M'.

Sea ahora M una matriz no nula arbitraria con entradas enteras, con s filas y k columnas y sea m el elemento no nulo de M con menor valor absoluto. Distinguimos dos casos:

Caso 1: m divide a todas las entradas de M. En ese caso, realizando si es necesario una operación elemental de tipo (iii) o (iii') podemos suponer que m es positivo y realizando operaciones elementales del tipo (i) y (i') podemos suponer que m es la primera entrada de M. Si $k = 1$ o $s = 1$, haciendo operaciones elementales de tipo (ii) o (ii') obtenemos una matriz con todas las entradas nulas excepto m y dicha matriz cumple los requisitos pedidos a M'. Si $k, s > 1$, haciendo operaciones elementales de tipo (ii) y (ii') obtenemos una matriz

$$\widehat{M} = \begin{pmatrix} m & 0 \\ 0 & \widetilde{M} \end{pmatrix},$$

donde 0 representa $k-1$ entradas nulas en la primera fila y $s-1$ entradas nulas en la primera columna y $\widetilde{M}$ es una matriz $(s-1)\times(k-1)$. Si $\widetilde{M}$ es la matriz nula, entonces $\widehat{M}$ cumple los requisitos pedidos a M' y ya hemos terminado. Si $\widetilde{M}$ no es la matriz nula, como tiene menos elementos que M, podemos aplicar la hipótesis de inducción sobre el número de elementos. Así pues, realizando operaciones elementales en $\widetilde{M}$, obtenemos una matriz $\widetilde{M'}$ que cumple los requisitos pedidos a M'. Entonces la matriz

$$\widehat{M'} = \begin{pmatrix} m & 0 \\ 0 & \widetilde{M'} \end{pmatrix},$$

se obtiene realizando operaciones elementales en $\widehat{M}$. Como el máximo común divisor de las entradas no nulas de una matriz no varía al realizar operaciones elementales m divide a todas la entradas no nulas de $\widetilde{M'}$ y, en particular, a la primera entrada de $\widetilde{M'}$. Por tanto, la matriz $\widehat{M'}$ cumple los requisitos pedidos a M'.

Caso 2: m no divide a todas las entradas de M.

Caso 2.1: Supongamos primero que existe alguna entrada m' de la primera fila o la primera columna de M que no es divisible por m'. Haciendo operaciones elementales de tipo (ii') o (ii) obtenemos una matriz con una entrada que tiene menor valor absoluto que m. Por ejemplo, si m' es la entrada de la primera fila i-ésima de la primera fila y no es divisible por m, hacemos la operación $C_i \to C_i - qC_1$, donde $m = m'q + m''$ es la división euclídea (véase el teorema 3.1.1) de m entre m', siendo q el cociente y r el resto de dicha división. En ese caso, después de realizar esa operación la entrada i-ésima de la primera fila se convierte en m'', que cumple $m'' < m$ (para un caso concreto puedes ver la tercera operación elemental del ejemplo 9.2.11).

Caso 2.2: Supongamos ahora que m divide a todas las entradas de la primera fila y la primera columna de M. Entonces existe una entrada $\tilde{m}$ que no está ni en la primera fila ni en la primera columna de M y que no es divisible por m. Si $\tilde{m}$ está en la fila j-ésima y en la columna i-ésima, consideramos la submatriz 2×2 de M formada por los elementos

en las posiciones $(1,1),(1,i),(j,1),(j,i)$,

$$M_{ji} = \begin{pmatrix} m & m_1 \\ m_2 & \tilde{m} \end{pmatrix},$$

donde m divide a m_1 y a m_2. Si hacemos por ejemplo $F_1 \to F_1 + F_j$, la matriz M_{ji} se transforma en

$$\begin{pmatrix} m+m_2 & m_1+\tilde{m} \\ m_2 & \tilde{m} \end{pmatrix}.$$

Como m divide a m_2, m también divide a $m+m_2$. Sin embargo $m+m_2$ no divide a $m_1+\tilde{m}$ pues, en caso contrario, m dividiría a $m_1+\tilde{m}$ y, como m divide a m_1, m también dividiría a $\tilde{m}$. Por tanto, realizando una operación elemental del tipo (ii) obtenemos una entrada m' (en lo anterior, $m' = m_1 + \tilde{m}$) en la primera fila que no es divisible por m (para un caso concreto, puedes ver la primera operación elemental del ejemplo 9.2.12). Así pues estamos en la situación del caso 2.1 y razonando como entonces obtenemos una matriz con una entrada $m'' < m$.

Así pues, tanto en el caso 2.1 como en el caso 2.2, haciendo operaciones elementales en M hemos obtenido otra matriz $\widehat{M}$ con una entrada m'' que tiene menor valor absoluto m. Aplicando la hipótesis de inducción sobre el mínimo del valor absoluto de los elementos de M concluimos que, haciendo operaciones elementales en $\widehat{M}$ obtenemos una matriz que cumple los requisitos pedidos a M'. □

A continuación usamos la proposición 9.2.13 para demostrar la existencia de la descomposición que aparece en (9.2.5.2). Como consecuencia del teorema chino del resto, a partir de dicha descomposición, obtendremos la descomposición primaria que aparece en (9.2.7.1):

Demostración de los teoremas 9.2.5 y 9.2.7, primera parte: existencia. Dado un grupo abeliano finitamente generado G consideramos una presentación de G (existe por la proposición 9.1.10) con matriz asociada M. Por la proposición 9.2.13, podemos, mediante operaciones elementales, obtener una matriz M' con ρ columnas y unos enteros no negativos $m_1,\dots,m_u$ como en (9.2.13.1). Entonces existen enteros no negativos s, $d_1,d_2,\dots,d_s$ tales que $d_1 > 1$ y los $m_1,\dots,m_u$ son $1,\dots,1,d_1,\dots,d_s$. Denotemos además $r = \rho - u$, que es un entero no negativo. Según la proposición 9.2.10, la matriz M' corresponde a una presentación de G. Por otra parte, la matriz M'' que obtenemos suprimiendo las filas nulas que pudiera haber en M' también corresponde a una presentación de G. Según la proposición 9.2.4, esa última presentación de G nos indica que G es isomorfo a

$$(\mathbf{Z}_{d_1} \times \mathbf{Z}_{d_2} \times \cdots \times \mathbf{Z}_{d_s} \times \mathbf{Z}^r, +)$$

y, por las condiciones que cumplen los $m_1,\dots,m_u$, se tiene que d_1 divide a d_2, d_2 divide a $d_3,\dots,d_{s_1}$ divide a d_s.

Sean ahora $q_1,\dots,q_k$ potencias positivas de números primos distintos, tales que $d_1 = q_1\cdots q_k$ es la descomposición de d_1 como producto de primos. Usando repetidamente el

teorema chino del resto deducimos que el anillo $(\mathbf{Z}_{d_1}, +, \cdot)$ es isomorfo al anillo

$$(\mathbf{Z}_{q_1} \times \cdots \times \mathbf{Z}_{q_k}, +, \cdot).$$

Haciendo el mismo argumento para $d_2, \ldots, d_s$, obtenemos potencias positivas $q_1, \ldots, q_t$, de números primos, no necesariamente distintos tales que el anillo

$$(\mathbf{Z}_{d_1} \times \mathbf{Z}_{d_2} \times \cdots \times \mathbf{Z}_{d_s} \times \mathbf{Z}^r, +, \cdot)$$

es isomorfo al anillo

$$(\mathbf{Z}_{q_1} \times \cdots \times \mathbf{Z}_{q_t} \times \mathbf{Z}^r, +, \cdot).$$

De esto se deduce que el grupo G es isomorfo al grupo

$$(\mathbf{Z}_{q_1} \times \cdots \times \mathbf{Z}_{q_t} \times \mathbf{Z}^r, +),$$

donde, como ya se ha dicho, $q_1, \ldots, q_t$ son potencias positivas de números primos, no necesariamente distintos. □

Para dar la demostración de la unicidad de los teoremas 9.2.5 y 9.2.7 necesitamos antes varias definiciones y resultados, principalmente la invariancia del rango de un grupo abeliano libre finitamente generado y del subgrupo de torsión de un grupo abeliano.

Proposición 9.2.14. *Sean r y r' números enteros no negativos y sea $\varphi : (\mathbf{Z}^r, +) \longrightarrow (\mathbf{Z}^{r'}, +)$ un homomorfismo de grupos. Si el homomorfismo φ es*

(1) inyectivo, entonces $r \leq r'$;

(2) sobreyectivo, entonces $r \geq r'$;

(3) un isomorfismo, entonces $r = r'$.

Demostración. Consideramos los espacios vectoriales $\mathbf{Q}^r$ y $\mathbf{Q}^{r'}$ sobre el cuerpo $\mathbf{Q}$. Sea $\{e_1, \ldots, e_r\}$ la base canónica de $\mathbf{Q}^r$ y sean $e'_1 := \varphi(e_1), \ldots, e'_r := \varphi(e_r)$. Sea φ inyectivo. Supongamos que $r > r'$. Como $r > r'$, $e'_1, \ldots, e'_r$ son vectores linealmente dependientes de $\mathbf{Q}^{r'}$, así que existen $\lambda_1, \ldots, \lambda_r \in \mathbf{Q}$, no todos nulos, tales que $\lambda_1 e'_1 + \cdots + \lambda_r e'_r = 0$. Quitando denominadores podemos suponer que $\lambda_1, \ldots, \lambda_r \in \mathbf{Z}$. Como φ es un homomorfismo de grupos, teniendo en cuenta la notación 9.1.6 se cumple

$$0 = \lambda_1 \varphi(e_1) + \cdots + \lambda_r \varphi(e_r) = \varphi(\lambda_1 e_1 + \cdots + \lambda_r e_r).$$

Como φ es inyectivo, $\lambda_1 e_1 + \cdots + \lambda_r e_r = 0$, pero entonces $e_1, \ldots, e_r$ serían linealmente dependientes en $\mathbf{Q}^r$, y esto es una contradicción ya que $\{e_1, \ldots, e_r\}$ son también la base canónica de $\mathbf{Q}^r$. La contradicción viene de suponer que $r > r'$, por lo que $r \leq r'$.

Supongamos ahora que φ es sobreyectivo. Sea u_j un elemento de la base canónica de $(\mathbf{Z}^{r'}, +)$. Entonces existen $\lambda_1, \ldots, \lambda_r \in \mathbf{Z}$ tales que

$$u_j = \varphi(\lambda_1 e_1 + \cdots + \lambda_r e_r) = \lambda_1 e'_1 + \cdots + \lambda_r e'_r.$$

Entonces $e'_1, \ldots, e'_r$ es un sistema de generadores de $\mathbf{Q}^{r'}$, por lo que $r \geq r'$.

Finalmente (iii) se sigue de (i) y de (ii). □

Definición 9.2.15. Sea $(G, \cdot)$ un grupo *no necesariamente abeliano ni finitamente generado* y sea $g \in G$.

(1) Decimos que g es un elemento *de torsión* de G si g tiene orden finito, es decir, si existe $m \in \mathbf{N}$ tal que $g^m = 1$.

(2) Decimos que G es de torsión si todo elemento de G es de torsión.

(3) Decimos que G está libre de torsión si el único elemento de torsión de G es el elemento neutro de G.

Observación 9.2.16. Si G es un grupo abeliano *no necesariamente finitamente generado*, el conjunto formado por todos los elementos de torsión de G es un subgrupo de G, ya que si g_1 y g_2 son tales que $g_1^{m_1} = g_2^{m_2} = 1$ para ciertos $m_1, m_2 \in \mathbf{N}$, entonces

$$(g_1 g_2^{-1})^{m_1 m_2} = (g_1^{m_1})^{m_2} (g_2^{m_2})^{-m_1} = 1.$$

En cambio, si G no es abeliano, los elementos de torsión de G no tiene porque ser un subgrupo de G, como prueba el ejercicio 9.

Definición 9.2.17. Sea G un grupo abeliano no necesariamente finitamente generado. Al subgrupo de G formado por todos sus elementos de torsión lo llamaremos *subgrupo de torsión* de G y lo denotaremos por $T(G)$.

Ejemplos 9.2.18. (1) Sea G un grupo no necesariamente abeliano. Si G es finito, entonces G es de torsión.

(2) Un grupo abeliano libre de rango r está libre de torsión.

(3) Los grupos $(\mathbf{R}, +)$ y $(\mathbf{C}, +)$ son grupos abelianos libres de torsión pero no son grupos abelianos finitamente generados. En efecto, si lo fueran serían isomorfos a $(\mathbf{Z}^r, +)$ para algún $r \in \mathbf{Z}$, por lo que serían conjuntos numerables y esto se falso.

(4) Los grupos $(\mathbf{Q}^*, \cdot)$, $(\mathbf{R}^*, \cdot)$ y $(\mathbf{C}^*, \cdot)$ no están libres de torsión ya que las raíces de la unidad son elementos de orden finito.

Proposición 9.2.19. *Sea G un grupo abeliano no necesariamente finitamente generado.*

(1) El grupo $G/T(G)$ está libre de torsión.

(2) Sea G el grupo

$$(\mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_l} \times \mathbf{Z}^r, +).$$

En ese caso $T(G) = \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_l} \times \{0\} \times \overset{r)}{\cdots} \times \{0\}$ y $G/T(G)$ es isomorfo a $\mathbf{Z}^r$.

Demostración. Denotemos $H = T(G)$. Sea $g \in G$, sea gH la clase de equivalencia de g en $G/T(G)$ y sea $n \in \mathbf{N}$. Entonces $(gH)^n = 1$ si y solo si $g^nH = 1$ y esto ocurre si y solo si $g^n \in H = T(G)$, por lo que g^n es de torsión. Existe entonces $m \in \mathbf{N}$ tal que $1 = (g^n)^m = g^{nm}$, por lo que $g \in T(G)$ y $gH = 1$. Esto quiere decir que el único elemento de torsión de $G/T(G)$ es el elemento neutro. Esto prueba (1).

Sea $n = n_1 n_2 \cdots n_l$. Si $v \in \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_l} \times \{0\} \times \overset{r)}{\cdots} \times \{0\}$, es claro que $nv = 0$ (nótese que estamos usando la notación aditiva 9.1.6). Consideramos ahora el homomorfismo sobreyectivo de grupos

$$\begin{array}{rccc} \pi: & G & \longrightarrow & \mathbf{Z}^r \\ & (v_1, v_2) & \mapsto & v_2, \end{array}$$

donde $v_1 \in \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_l}$ y $v_2 \in \mathbf{Z}^r$. El núcleo de π es $T(G)$, así que concluimos el argumento usando el teorema 6.3.3. □

Proposición 9.2.20. *Sean G y G' dos grupos, no necesariamente abelianos ni necesariamente finitamente generados y sea φ un isomorfismo de grupos entre G y G'.*

(1) El orden del elemento g de G es el orden de $\varphi(g)$ en G'.

(2) La imagen por φ del conjunto formado por los elementos de torsión de G es el conjunto formado por los elementos de torsión de G'.

(3) Si G y G' son abelianos, entonces φ induce un isomorfismo entre $T(G)$ y $T(G')$ y entre $G/T(G)$ y $G'/T(G')$.

Demostración. Sea $g \in G$ un elemento de orden finito sea n el orden de g. Si φ es un homomorfismo, no necesariamente inyectivo,

$$(\varphi(g))^n = \varphi(g^n) = \varphi(1_G) = 1_{G'}, \tag{9.2.20.1}$$

por lo que $\varphi(g)$ es un elemento de orden finito de G'. Sea m el orden de $\varphi(g)$. Por la proposición 5.4.8 m divide a n. Si φ es un isomorfismo, aplicando lo anterior a φ^{-1} obtenemos que el orden de $g = \varphi^{-1}(\varphi(g))$ divide al orden de $\varphi(g)$, de donde $n = m$.

Por el apartado (1), $g \in G$ tiene orden finito, es decir, es un elemento de torsión de G si y solo si $\varphi(g) \in G'$ tiene orden finito, es decir, es un elemento de torsión de G'. Esto demuestra (2).

Si G y G' son abelianos, $T(G)$ es subgrupo de G y $T(G')$ es subgrupo de G'. Como la restricción de φ a $T(G)$ es inyectiva y, por el apartado (2), $\varphi(T(G)) = T(G')$, la restricción de φ a $T(G)$ es un isomorfismo de grupos entre $T(G)$ y $T(G')$. Como G y G' son abelianos, $T(G)$ y $T(G')$ son subgrupos normales de G y G' respectivamente, por lo que podemos considerar los grupos cocientes $G/T(G)$ y $G'/T(G')$. Sea $\pi' : G' \longrightarrow G'/T(G')$ la proyección canónica y sea $\varphi' = \pi' \circ \varphi$. Como φ es un isomorfismo y π' es sobreyectivo, tenemos que φ' es sobreyectivo. Por otro lado, de (2) se sigue que el núcleo de φ' es

$$\varphi'^{-1}(1_{G'}) = \varphi^{-1}(\pi'^{-1}(1_{G'}) = \varphi^{-1}(T(G')) = T(G).$$

Aplicando a φ' el teorema 6.3.3, tenemos que

$$\begin{array}{rccc} \overline{\varphi'}: & G/T(G) & \longrightarrow & G'/T(G') \\ & gT(G) & \mapsto & \varphi(g)T(G') \end{array}$$

es un isomorfismo de grupos. □

Lema 9.2.21. *Sean G_1, G_2, G_1', G_2' grupos* no necesariamente abelianos ni finitamente generados *y sea*

$$\varphi : G_1 \times G_2 \longrightarrow G_1' \times G_2'$$

un isomorfismo de grupos tal que

$$\varphi(< 1_{G_1} > \times G_2) =< 1_{G_1'} > \times G_2'.$$

Entonces G_1 y G_1' son isomorfos.

Demostración. Consideramos la aplicación

$$\begin{array}{rccc} \pi: & G_1' \times G_2' & \longrightarrow & G_1' \\ & (g_1', g_2') & \mapsto & g_1'. \end{array}$$

Es claro que π es un homomorfismo de grupos sobreyectivo cuyo núcleo es $< 1_{G_1'} > \times G_2'$. Sea $\varphi' = \pi \circ \varphi$. El núcleo de φ' es $\varphi^{-1}(\operatorname{Ker}\pi) = \varphi^{-1}(< 1_{G_1'} > \times G_2')$, que es $< 1_{G_1} > \times G_2$ por ser φ isomorfismo y cumplir $\varphi(< 1_{G_1} > \times G_2) =< 1_{G_1'} > \times G_2'$. La conclusión se sigue entonces del teorema 6.3.3 y de la proposición 9.1.3 (4). □

Ya estamos listos para demostrar la unicidad en los teoremas 9.2.5 y 9.2.7:

Demostración de los teoremas 9.2.5 y 9.2.7; segunda parte: unicidad. Consideramos los grupos

$$G = (\mathbf{Z}_{q_1} \times \cdots \times \mathbf{Z}_{q_t} \times \mathbf{Z}^r, +) \tag{9.2.21.1}$$

y

$$G' = (\mathbf{Z}_{q_1'} \times \cdots \times \mathbf{Z}_{q_{t'}'} \times \mathbf{Z}^{r'}, +) \tag{9.2.21.2}$$

donde los q_i y los q_j' son potencias de primos no necesariamente distintas y supongamos que son isomorfos.

Paso 1: Por la proposición 9.2.20, los subgrupos de torsión $T(G)$ y $T(G')$ son isomorfos y por las proposiciones 9.2.19 (2) y 9.2.20, $(\mathbf{Z}^r, +)$ y $(\mathbf{Z}^{r'}, +)$ también son isomorfos. Entonces Por la proposición 9.2.14 (3), $r = r'$.

Paso 2: Por la proposición 9.2.19 (2),

$$T(G) \simeq (\mathbf{Z}_{q_1} \times \cdots \times \mathbf{Z}_{q_t}, +)$$

y

$$T(G') \simeq (\mathbf{Z}_{q_1'} \times \cdots \times \mathbf{Z}_{q_{t'}'}, +).$$

Haciendo un abuso de notación llamaremos $T(G)$ a $(\mathbf{Z}_{q_1} \times \cdots \times \mathbf{Z}_{q_t}, +)$ y $T(G')$ a $(\mathbf{Z}_{q'_1} \times \cdots \times \mathbf{Z}_{q'_{t'}}, +)$. Por el paso 1, $T(G)$ y $T(G')$, son isomorfos. Sea p uno de los primos que aparece en las potencias $q_1, \ldots, q_t$. Entonces existe un elemento de $T(G)$ cuyo orden es una potencia de p. Por la proposición 9.2.20, existe un elemento de $T(G')$ cuyo orden también es una potencia de p, por lo que p aparece en las potencias $q'_1, \ldots, q'_{t'}$. Razonando de esta forma para todos los primos que aparecen en las potencias $q_1, \ldots, q_t$ y en las potencias $q'_1, \ldots, q'_{t'}$, concluimos que los primos que aparecen en $q_1, \ldots, q_t$ y $q'_1, \ldots, q'_{t'}$ son los mismos.

Paso 3: Agrupamos los factores de $T(G)$ y $T(G')$ que corresponden a potencias del mismo primo. Fijamos uno de esos primos p. Sean G_p (respectivamente G'_p) el subgrupo de G (respectivamente de G') formado por aquellos elementos de G que tienen nulas las entradas que corresponden a factores $\mathbf{Z}_{q_i}$ en los que p no divide a q_i (respectivamente por aquellos elementos de G' que tienen nulas las entradas que corresponden a factores $\mathbf{Z}_{q'_j}$ en los que p no divide a q'_j). El teorema 5.5.9 y el ejercicio 10 del tema 5 implican que G_p (respectivamente G'_p) está formado por los elementos de G cuyo orden es una potencia de p (respectivamente por los elementos de G' cuyo orden es una potencia de p). Entonces la proposición 9.2.20 implica que G_p y G'_p son isomorfos. Como hay un isomorfismo natural de G_p al producto de los factores de $T(G)$ correspondientes a potencias de p, haciendo un abuso de notación llamaremos G_p a dicho producto y haremos lo análogo para G'_p. La proposición 9.2.20 implica también que el máximo de los órdenes de los elementos de G_p y G'_p coincide, llamémosle p^l. Entonces

$$G_p = \mathbf{Z}_{p^{l_1}} \times \cdots \times \mathbf{Z}_{p^{l_c}} \times \mathbf{Z}_{p^l}$$
$$G'_p = \mathbf{Z}_{p^{n_1}} \times \cdots \times \mathbf{Z}_{p^{n_{c'}}} \times \mathbf{Z}_{p^l},$$

donde $1 \leq l_1 \leq \cdots \leq l_c \leq l$ y $n_1 \leq \cdots \leq n_{c'} \leq l$. Vamos a demostrar, por inducción sobre el número de factores de G_p, que $c = c'$ y que $l_1 = n_1$, $l_2 = n_2$ y así hasta $l_c = n_{c'}$. Si G_p tiene solo un factor, entonces $G_p = \mathbf{Z}_{p^l}$. Como G_p y G'_p son isomorfos, G'_p tiene p^l elementos, por lo que $c' = 0 = c$. Consideremos ahora $c \leq 1$. Denotemos

$$\widetilde{G}_p := \mathbf{Z}_{p^{l_1}} \times \cdots \times \mathbf{Z}_{p^{l_c}}$$
$$\widetilde{G}'_p := \mathbf{Z}_{p^{n_1}} \times \cdots \times \mathbf{Z}_{p^{n_{c'}}}.$$

Queremos usar el lema 9.2.21, por lo que necesitamos probar que existe un isomorfismo entre G_p y G'_p que transforme $< 0_{\widetilde{G}_p} > \times \mathbf{Z}_{p^l}$ en $< 0_{\widetilde{G}'_p} > \times \mathbf{Z}_{p^l}$. Sea φ un isomorfismo cualquiera entre G_p y G'_p. Consideramos el elemento $v = (0, \ldots, 0, 1)$ de G_p. Como v tiene orden p^l, se sigue de la proposición 9.2.20 que $w' := \varphi(v)$ también tiene orden p^l. Entonces, por la proposición 5.4.6, el ejemplo 5.4.11 y el corolario 5.5.10, podemos suponer que la última coordenada del "vector" w' de G'_p es $\overline{\alpha} \in \mathbf{Z}_{p^l}$, con α y p primos entre sí. Consideramos los elementos $w_1 := (1, 0, \ldots, 0), \ldots, w_{c'} := (0, \ldots, 0, 1, 0)$ y $w = (0, \ldots, 0, 1)$ de G'_p. Entonces

$$w' = \alpha_1 w_1 + \cdots + \alpha_c w_c + \alpha w, \tag{9.2.21.3}$$

con $\alpha_1, \ldots, \alpha_c, \alpha \in \mathbf{Z}$ y α y p primos entre sí. El conjunto $\{w_1, \ldots, w_c, w'\}$ es un sistema de generadores de G'_p, ya que $w = \beta(w' - \alpha_1 w_1 - \cdots - \alpha_c w_c)$, donde β es el inverso de α módulo p^l, por lo que cada $w_1, \ldots, w_c, w$ es una combinación de $w_1, \ldots, w_c, w'$ con coeficientes enteros. Por el lema 9.1.9 existe un homomorfismo sobreyectivo de grupos ψ entre $\mathbf{Z}^{c+1}$ y G'_p que cumple $\psi(e_1) = w_1, \ldots, \psi(e_c) = w_c, \psi(e_{c+1}) = w'$, donde $\{e_1, \ldots, e_c, e_{c+1}\}$ es la base canónica de $\mathbf{Z}^{c+1}$. Estudiamos ahora el núcleo de ψ. Sean $\gamma_1, \ldots, \gamma_c, \gamma_{c+1}$ en $\mathbf{Z}$ y sea $\rho = \gamma_1 e_1 + \cdots + \gamma_c e_c + \gamma_{c+1} e_{c+1}$ un elemento del núcleo de ψ. Entonces

$$0 = \psi(\rho) = \gamma_1 \psi(e_1) + \cdots + \gamma_c \psi(e_c) + \gamma_{c+1} \psi(e_{c+1}) = \gamma_1 w_1 + \cdots + \gamma_c w_c + \gamma_{c+1} w'.$$

En ese caso $\gamma_1, \ldots, \gamma_c, \gamma_{c+1}$ satisfacen el siguiente sistema de congruencias:

$$\begin{array}{ccc} \gamma_1 + \alpha_1 \gamma_{c+1} & \equiv & 0 \text{ mód } p^{n_1} \\ \vdots & \vdots & \vdots \\ \gamma_c + \alpha_c \gamma_{c+1} & \equiv & 0 \text{ mód } p^{n_{c'}} \\ \alpha \gamma_{c+1} & \equiv & 0 \text{ mód } p^l \end{array} \tag{9.2.21.4}$$

Recordemos que, como α y p son primos entre sí, α tiene inverso módulo p; multiplicando la última congruencia por el inverso de α obtenemos que γ_{c+1} es congruente con 0 módulo p^l. Como l es mayor o igual que $n_1, \ldots, n_{c'}$, las potencias $p^{n_1}, \ldots, p_{n_{c'}}$ dividen a p^l, de donde γ_{c+1} es congruente con 0 módulo p^{n_1}, módulo p^{n_2} y así hasta módulo $p_{n_{c'}}$. Así pues del sistema (9.2.21.4) llegamos al sistema

$$\begin{array}{ccc} \gamma_1 & \equiv & 0 \text{ mód } p^{n_1} \\ \vdots & \vdots & \vdots \\ \gamma_c & \equiv & 0 \text{ mód } p^{n_{c'}} \\ \gamma_{c+1} & \equiv & 0 \text{ mód } p^l \end{array}$$

es decir, γ_1 es múltiplo de p^{n_1}, γ_2 es múltiplo de p^{n_2} y así hasta γ_c, que es múltiplo de $p^{n_{c'}}$ y γ_{c+1}, que es múltiplo de p^l. Entonces el núcleo de ψ está generado por $p^{n_1} e_1, \ldots, p^{n_{c'}} e_c, p^l e_{c+1}$. La proposición 9.2.4 nos dice entonces que el cociente de $\mathbf{Z}^{c+1}$ por el núcleo de ψ es isomormo a $\mathbf{Z}_{p^{n_1}} \times \cdots \times \mathbf{Z}_{p^{n_{c'}}} \times \mathbf{Z}_{p^l}$ y el teorema 6.3.3 nos dice que existe un isomorfismo de grupos

$$\overline{\psi} : \mathbf{Z}_{p^{n_1}} \times \cdots \times \mathbf{Z}_{p^{n_{c'}}} \times \mathbf{Z}_{p^l} \longrightarrow G'_p$$

que cumple $\overline{\psi}(0, \ldots, 0, 1) = w'$, es decir, un isomorfismo de grupos

$$\overline{\psi} : G'_p \longrightarrow G'_p$$

que cumple $\overline{\psi}(w) = w'$. Sea ahora $\varphi' = \overline{\psi}^{-1} \circ \varphi$. La aplicación φ' es un isomorfismo de G_p a G'_p que cumple $\varphi'(v) = w$. Como $< 0_{\widetilde{G}_p} > \times \mathbf{Z}_{p^l}$ es un subgrupo cíclico de $G_p = \widetilde{G}_p \times \mathbf{Z}_{p^l}$

generado por v y $< 0_{\widetilde{G}_p'} > \times \mathbf{Z}_{p^l}$ es un subgrupo cíclico de $G_p' = \widetilde{G}_p' \times \mathbf{Z}_{p^l}$ generado por w, tenemos que

$$\varphi'(< 0_{\widetilde{G}_p} > \times \mathbf{Z}_{p^l}) =< 0_{\widetilde{G}_p'} > \times \mathbf{Z}_{p^l}.$$

El lema 9.2.21 nos dice entonces que $\widetilde{G}_p$ y $\widetilde{G}_p'$ son grupos isomorfos. Como $\widetilde{G}_p$ tiene un factor menos que G_p, se sigue de la hipótesis de inducción que $c = c'$ y que $l_1 = n_1$, $l_2 = n_2$ y así hasta $l_c = n_{c'}$.

Sintetizamos lo visto en los pasos 1, 2 y 3. Si los grupos G y G' (veáse (9.2.21.1) y (9.2.21.2) son isomorfos, el paso 1 nos dice que tienen el mismo rango, es decir, que $r = r'$. El paso 2 nos dice que los primos correspondientes a los factores de torsión que aparecen en las descomposiciones de G y G' son los mismos, es decir, que los primos que aparecen en $q_1, \ldots, q_t$ son los mismos que los que aparecen en $q_1', \ldots, q_{t'}'$ son los mismos. El paso 3 nos dice que, para cada uno de esos primos p, las potencias de p en la lista $q_1, \ldots, q_t$ son las mismas que las potencias de p en la lista $q_1', \ldots, q_{t'}'$ y también son las mismas las veces que se repite una potencia dada de p en ambas listas. Por tanto $\{q_1, \ldots, q_t\}$ y $\{q_1', \ldots, q_{t'}'\}$ y, en particular $t = t'$. Esto junto con $r = r'$ quiere decir que, si ordenamos los $q_1, \ldots, q_t$ y los $q_1', \ldots, q_t'$ para que cumplan (i) y (ii) del enunciado del teorema 9.2.7, entonces las descomposiciones (9.2.21.1) y (9.2.21.2) son la misma. Esto completa la demostración de la unicidad en el teorema 9.2.7. Como ya se ha demostrado en el paso 1 que el rango de un grupo abeliano finitamente generado es invariente por isomorfismo, para demostrar la unicidad en el teorema 9.2.5 basta probar la unicidad de los coeficientes de torsión de un grupo abeliano finitamente generado:

Paso 4: Sea G un grupo abeliano finitamente generado. Dada la descomposición primaria de $T(G)$ que aparece en (9.2.21.1), los coeficientes de torsión de $T(G)$ se determinan de manera única a partir de las potencias $q_1, \ldots, q_t$ por el siguiente procedimiento. Ordenamos los números $q_1, \ldots, q_t$ colocándolos en una "tabla" con s filas de manera que

(i) en la primera columna de la tabla estén las potencias del primo más pequeño, en la segunda columna de la tabla estén las potencias del siguiente primo más pequeño y así sucesivamente;

(ii) en la primera casilla de la columna correspondiente a un primo p esté la potencia más grande $q_k = p^l$ de p que aparece en la lista $q_1, \ldots, q_t$; en la segunda casilla (inmediatamente inferior) esté la mayor potencia de p que aparece en la lista $q_1, \ldots, q_{k-1}, q_{k+1}, \ldots, q_t$ (ten en cuenta que dicha potencia podría ser otra vez p^l, ya que los elementos de la lista $q_1, \ldots, q_t$ no son necesariamente distintos) y así sucesivamente y evitando en particular dejar huecos en la columna.

A partir de la tabla obtenemos una lista $d_1, \ldots, d_s$ de números de esta forma: d_i es el producto de los números en la fila $s + 1 - i$-ésima de la tabla. Observa que la condición (ii) impuesta a la tabla es necesaria y suficiente para que $d_1, \ldots, d_s$ cumplan (9.2.5.1). Observa también que las condiciones (i) y (ii) determinan una única tabla a partir de

$q_1, \ldots, q_t$. Del corolario 3.4.11 y de la demostración del corolario 5.4.8 se sigue que

$$\mathbf{Z}_{q_1} \times \cdots \times \mathbf{Z}_{q_t} \simeq \mathbf{Z}_{d_1} \times \cdots \times \mathbf{Z}_{d_s}.$$

Sea ahora G' un grupo abeliano finitamente generado isomorfo a G'. Entonces $T(G)$ es isomorfo a $T(G')$ y, por la unicidad en el teorema 9.2.7, $q_1, \ldots, q_t$ es la única lista (no ordenada) de potencias de números primos tal que

$$T(G') \simeq \mathbf{Z}_{q_1} \times \cdots \times \mathbf{Z}_{q_t}.$$

Por la unicidad de la tabla construida a partir de $q_1, \ldots, q_s$ y por el corolario 3.4.11 y la demostración del corolario 5.4.8, los únicos números naturales $d'_1, \ldots, d'_{s'}$, mayores que 1 tales que

$$T(G') \simeq \mathbf{Z}_{d'_1} \times \cdots \times \mathbf{Z}_{d'_{s'}}$$

que cumplen (9.2.5.1) son $d'_1 = d_1, \ldots, d'_{s'} = d_s$ (y, en particular, $s = s'$). □

Ejemplo 9.2.22. Consideramos en grupo abeliano finito

$$G = \mathbf{Z}_2 \times \mathbf{Z}_8 \times \mathbf{Z}_9 \times \mathbf{Z}_5 \times \mathbf{Z}_5 \times \mathbf{Z}_{25} \times \mathbf{Z}_7 \tag{9.2.22.1}$$

(1) A la descomposición primaria (9.2.22.1) de G le corresponde la tabla

8	9	25	7
2		5	
		5	

que cumple las condiciones (i) y (ii) del paso 4 de la demostración de la unicidad de los teoremas 9.2.5 y 9.2.7. Siguiendo los argumentos del paso 4, obtenemos la lista de números naturales $5, 10, 12600$, que cumple (9.2.5.1), de manera que G es isomorfo a $\mathbf{Z}_5 \times \mathbf{Z}_{10} \times \mathbf{Z}_{12600}$, es decir, la descomposición en factores invariantes de G es $\mathbf{Z}_5 \times \mathbf{Z}_{10} \times \mathbf{Z}_{12600}$.

(2) La tabla

8	9	5	7
2		25	
		5	

en cambio no cumple la condición (ii) del paso 4 de la demostración de la unicidad de los teoremas 9.2.5 y 9.2.7 y, en consecuencia, la lista de números naturales $5, 50, 2520$ no cumple (9.2.5.1), por lo que, aunque, por el corolario 3.4.11, G es isomorfo a $\mathbf{Z}_5 \times \mathbf{Z}_{50} \times \mathbf{Z}_{2520}$, esta no es una descomposición de G en factores invariantes.

Como consecuencia del teorema 9.2.5 obtenemos los siguientes resultados:

Corolario 9.2.23. *Sea G un grupo abeliano finitamente generado.*

(1) G es libre si y solo si G está libre de torsión.

(2) Si G es libre, entonces todo subgrupo de G es libre.

Demostración. Vimos en el ejemplo 9.2.18 (2) que, si G es libre, entonces G es libre de torsión. Si G es libre de torsión por el teorema 9.2.5 y por la proposición 9.2.19, se tiene que G es isomorfo a $\mathbf{Z}^r$ para algún $r \in \mathbf{N}$. Esto completa la prueba de (1).
Sea H un subgrupo de G. El subgrupo H no tiene torsión porque G es libre y, por tanto, sin torsión. Por la proposición 9.1.12, H está finitamente generado, así que (2) se sigue de (1). □

Corolario 9.2.24. *Si F es un cuerpo finito, su grupo de unidades es cíclico.*

Demostración. Resuelve el ejercicio 5 del tema 9. □

Apéndice: Clases y conjunto cociente de una relación de equivalencia

Sea A un conjunto y sea $\sim$ una relación de equivalencia en A (es decir, $\sim$ cumple las propiedades reflexiva, simétrica y transitiva). Recordamos las definiciones y hechos siguientes:

(1) Sea $a \in A$. La *clase de equivalencia* de a, que denotamos a aquí por $[a]$ es

$$[a] = \{a' \in A \mid a \sim a'\}.$$

(2) El *conjunto cociente* de $\sim$, que denotamos por $A/\!\sim$ es el conjunto formado por las clases de equivalencia de todos los elementos de A, es decir,

$$A/\!\sim = \{\, [a] \mid a \in A\}.$$

(3) Las clases de equivalencia de elementos distintos de A pueden ser iguales, es decir, elementos distintos de A pueden dar lugar al mismo elemento del cociente. El resultado preciso es el siguiente:

Sean $a, b \in A$. Entonces $a \sim b$ si y solo si $[a] = [b]$ si y solo si $a \in [b]$ si y solo si $b \in [a]$.

(4) A es la unión disjunta de todas las clases de equivalencia de A. Por tanto, dadas dos clases de equivalencia $[a]$ y $[b]$, o bien $[a] = [b]$, o bien $[a] \cap [b] = \emptyset$. En particular, si $a \not\sim b$ si y solo si $[a] \neq [b]$ si y solo si $[a] \cap [b] = \emptyset$.

Ejemplo A.1. Sea n un número natural. En $A = \mathbf{Z}$ consideramos la siguiente relación: dados $m_1, m_2 \in \mathbf{Z}$, $m_1 \sim m_2$ si y solo si m_1 y m_2 tienen el mismo resto (entre 0 y $n-1$) al dividir por n. La relación $\sim$ es una relación de equivalencia y se llama *relación de congruencia módulo n*. Si $m_1 \sim m_2$ decimos que m_1 y m_2 son congruentes módulo n y escribimos $m_1 \equiv m_2 (n)$ o $m_1 \equiv m_2$ mód n.

Es claro que

$$\mathbf{Z} = [0] \sqcup [1] \sqcup [2] \sqcup \cdots \sqcup [n-1]$$

($\sqcup$ quiere decir unión disjunta), ya que todo número entero tiene un único resto, entre 0 y $n-1$, al dividir por n.