ESTRUCTURAS ALGEBRAICAS

FERNANDO MURO

Resumen. Notas de la asignatura Estructuras Algebraicas del Grado en Matemáticas de la Universidad de Sevilla. Esta versión en PDF se ha generado automáticamente a partir de la página web `http://asignatura.us.es/estalg/` y puede contener errores derivados del proceso de conversion. Les agradecería que informasen de cualquier error que encuentren escribiendo a `fmuro@us.es`.

Índice

Parte 1. Anillos

Consideremos la ecuación

$$x^2 - y^2 = 25.$$

Nos proponemos hallar todas sus soluciones enteras, $x, y \in \mathbb{Z}$. El miembro de la izquierda se puede factorizar como producto de dos enteros y el de la derecha como producto de primos,

$$(x+y)(x-y) = 5^2.$$

El **teorema fundamental de la aritmética** asegura que todo entero se descompone como producto de primos de manera única salvo signo. Por tanto, para que esta última ecuación sea cierta es necesario que los factores primos de 25 se repartan entre los dos términos de la izquierda, de nuevo salvo signo. Es decir, las soluciones a nuestro problema son las soluciones enteras de los siguientes seis sistemas de ecuaciones lineales,

$$\left\{ \begin{array}{rcrrrrrr} x+y & = & 1, & -1, & 5, & -5, & 25, & -25; \\ x-y & = & 25, & -25, & 5, & -5, & 1, & -1. \end{array} \right.$$

Todos ellos son compatibles determinados y su solución es entera,

$$\begin{array}{rcl} (x,y) & = & (13,-12),\ (-13,12),\ (5,0), \\ & & (-5,0),\ (13,12),\ (-13,-12). \end{array}$$

Ahora introduciremos ligeros cambios en nuestra ecuación y consideraremos

$$x^2 + y^2 = 5.$$

En este caso no podemos obtener una factorización general no trivial del término de la izquierda como producto de dos enteros. Podemos sin embargo considerar factorizaciones en el **anillo** $\mathbb{Z}[i]$ de los números complejos con partes real e imaginaria enteras, denominados **enteros de Gauss**. Aquí los miembros de la ecuación factorizan como

$$(x+iy)(x-iy) = (2+i)(2-i).$$

En este capítulo veremos, entre otras muchas cosas, que el teorema fundamental de la aritmética también tiene sentido en $\mathbb{Z}[i]$. Cualquier entero de Gauss se descompone como producto de primos de manera única, no solo salvo signo sino salvo producto por $\{\pm 1, \pm i\}$, que son los enteros de Gauss invertibles. Además, 5 no es primo en $\mathbb{Z}[i]$ y su descomposición como producto de primos es el término de la derecha de la última ecuación.

El razonamiento anterior nos conduce a que las soluciones de la ecuación que nos ocupa son las soluciones enteras de los siguientes dieciséis sistemas de ecuaciones lineales,

$$\left\{\begin{array}{rcrrrr} x+iy & = & 1, & -1, & i, & -i, \\ x-iy & = & 5, & -5, & -i5, & i5, \end{array}\right.$$

$$\left\{\begin{array}{rcrrrr} x+iy & = & (2+i), & -(2+i), & i(2+i), & -i(2+i), \\ x-iy & = & (2-i), & -(2-i), & -i(2-i), & i(2-i), \end{array}\right.$$

$$\left\{\begin{array}{rcrrrr} x+iy & = & (2-i), & -(2-i), & i(2-i), & -i(2-i), \\ x-iy & = & (2+i), & -(2+i), & -i(2+i), & i(2+i), \end{array}\right.$$

$$\left\{\begin{array}{rcrrrr} x+iy & = & 5, & -5, & i5, & -i5; \\ x-iy & = & 1, & -1, & -i, & i. \end{array}\right.$$

Como los térmios de la izquierda, $x+iy$ y $x-iy$, son conjugados, podemos descartar de plano los sistemas cuyos términos independientes no lo sean, es decir, los cuatro primeros y los cuatro últimos. Las soluciones del resto, y de nuestro problema, son

$$\begin{array}{rcl} (x,y) & = & (2,1),\,(-2,-1),\,(-1,2),\,(1,-2), \\ & & (2,-1),\,(-2,1),\,(1,2),\,(-1,-2). \end{array}$$

Obviamente nuestra segunda ecuación se puede resolver fácilmente por métodos elementales, pero los métodos expuestos en este ejemplo, y otros aún más sofisticados, nos permitirán resolver otras ecuaciones que ahora no están realmente a nuestro alcance.

1.1. Definiciones

Recuerda que un **anillo** R es un conjunto donde están definidas las siguientes operaciones para $a, b \in R$:

- **suma**: $a+b$,
- **multiplicación** o **producto**: ab,

y además existen elementos:

- **cero**: 0,
- **uno**: 1,

que satisfacen las propiedades habituales de asociatividad y distributividad. La debe ser conmutativa y en esta asignatura solo consideraremos anillos donde el producto también lo es. Todos los elementos a han de poseer **opuestos** para la suma $-a$, con lo cual podemos restar. Los que poseen inversos para el producto se denominan **unidades** y podemos dividir por ellos. Un **cuerpo** es un anillo donde $0 \neq 1$ y todo elemento no nulo es una unidad. Se puede comprobar que $0 = 1$ en un anillo R si y solo si $R = \{0\}$ es el anillo trivial.

Ejemplos de anillos son:

- Los números enteros $\mathbb{Z}$, racionales $\mathbb{Q}$, reales $\mathbb{R}$ y complejos $\mathbb{C}$, pero no los naturales $\mathbb{N}$.
- El anillo de polinomios $R[x]$ en una variable x con coeficientes en un anillo R.
- El anillo de polinomios en varias variables $R[x_1, \ldots, x_n]$, que se puede definir inductivamente como $R[x_1, \ldots, x_{n-1}][x_n]$.
- El álgebra de Boole de las partes de un conjunto.
- El anillo de funciones continuas $\mathcal{C}(X, \mathbb{R})$ definidas en un espacio topológico X con valores reales. También lo es su versión con valores complejos $\mathcal{C}(X, \mathbb{C})$ y, cuando la naturaleza de X le dé sentido, lo anillos de funciones derivables, analíticas, etc.

El **producto** cartesiano $R \times S$ de dos anillos R y S es un anillo con las operaciones definidas por coordenadas. El cero y el uno del producto son $(0, 0)$ y $(1, 1)$.

Recuerda también que un **subanillo** $R' \subset R$ de un anillo R es un subconjunto cerrado para la suma y el producto que contiene al 1 y a los opuestos de todos sus elementos. Podemos ver $R \subset R[x]$ como el subanillo de los polinomios constantes, sin embargo $R \times \{0\} \subset R \times S$ en general no es un subanillo. El total $R \subset R$ siempre es un subanillo pero $\{0\} \subset R$ generalmente no.

1.1.1. El principio de sustitución. Recuerda que un **homomorfismo** de anillos $f\colon R \to S$ es una aplicación que preserva esta estructura, es decir la suma, el producto, el 0 y el 1. Los homomorfismos inyectivos se denominan **monomorfismos**, los sobreyectivos **epimorfismos** y los biyectivos **isomorfismos**. Estos últimos se denotan con el símbolo $\cong$. Los isomorfismos de un anillo en sí mismo reciben el nombre de **automorfismos**.

Todas estas clases de morfismos son cerradas para la composición y contienen a la identidad. Es más, el inverso de un isomorfismo es también un isomorfismo, e igual para automorfismos. La conjugación compleja es un automorfismo no trivial de $\mathbb{C}$. El inverso de un isomorfismo también es un isomorfismo. La inclusión de un subanillo $R' \hookrightarrow R$ es un monomorfismo y la proyección sobre la primera coordenada $R \times S \twoheadrightarrow R$ es un epimorfismo, sin embargo estos, en general, no son isomorfismos. Se da el hecho curioso de que, para todo anillo R, existe un único homomorfismo $\mathbb{Z} \to R$, es decir, $\mathbb{Z}$ es el objeto incial en la categoría de los anillos.

Los homomorfismos preservan las unidades y sus inversos. La **imágen** de un homomorfismo $f\colon R \to S$ es un subanillo $\operatorname{im} f \subset S$.

Dado un anillo R y $a \in R$ está definido el homomorfismo de **evaluación** $ev_a\colon R[x] \to R$ como $ev_a(p(x)) = p(a)$. Los anillos de polinomios satisfacen una propiedad universal relacionada con estos homomorfismos.

Teorema 1.1.1.1. (Principio de sustitución) *Dado un homomorfismo de anillos $f\colon R \to S$ y un elemento $c \in S$ existe un único homomorfismo $g\colon R[x] \to S$ tal que la restricción de g a R es f y $g(x) = c$.*

Demostración. Dado $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$, si tal $g\colon R[x] \to S$ existiera satisfaría

$$\begin{aligned} g(p(x)) &= g(a_n x^n + \cdots + a_1 x + a_0) \\ &= g(a_n) g(x)^n + \cdots + g(a_1) g(x) + g(a_0) \\ &= f(a_n) c^n + \cdots + f(a_1) c + f(a_0). \end{aligned}$$

Definimos pues

$$g(p(x)) = f(a_n)c^n + \cdots + f(a_0).$$

Es tedioso pero trivial comprobar g así definido es un homomorfismo. El cálculo anterior demuestra la unicidad. □

Corolario 1.1.1.2. *Dado un homomorfismo de anillos $f\colon R \to S$ y elementos $c_1, \ldots, c_n \in S$ existe un único homomorfismo $g\colon R[x_1, \ldots, x_n] \to S$ tal que la restricción de g a R es f y $g(x_i) = c_i$, $1 \leq i \leq n$.*

Demostración. Se puede demostrar directamente como el teorema anterior, pero también se puede probar a partir de él por inducción en n.

Para $n = 1$, la existencia y unicidad de $g\colon R[x_1] \to S$ es el teorema anterior.

Veamos que $n-1 \Rightarrow n$. Suponiendo que hay un único homomorfismo $h\colon R[x_1, \ldots, x_{n-1}] \to S$ que se restringe a $f\colon R \to S$ sobre las constantes y satisface $g(x_i) = c_i$, $1 \leq i \leq n-1$, aplicamos el teorema anterior a

$$R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$$

y obtenemos el homomorfismo buscado.

□

1.1.2. Añadir elementos a un anillo. La siguiente definición nos da una receta para añadir nuevos elementos a un anillo contenido en otro mayor.

Definición 1.1.2.1. Dado un anillo S, un subanillo $R \subset S$ y $s \in S$, el menor subanillo $R[s] \subset S$ que contiene a R y a s es la imagen del homomorfismo $g\colon R[x] \to S$ definido como la inclusión $i\colon R \hookrightarrow S$ sobre R tal que $g(x) = s$, $R[s] = \operatorname{im} g$.

Observación 1.1.2.2. La propiedad de ser el menor viene dada porque todo elemento de $R[s]$ se puede expresar (aunque no de manera única) como $a_n s^n + \cdots + a_1 s + a_0$ para ciertos $a_i \in R$. Por tanto, si $U \subset S$ es un subanillo tal que $R \subset U$ y $s \in U$ entonces $R[s] \subset U$. En particular $\mathbb{R}[i] = \mathbb{C}$ y $\mathbb{Z}[i] \subset \mathbb{C}$ son los enteros de Gauss.

Ejercicio 1.1.2.3. Da una definición directa del menor subanillo $R[s_1, \ldots, s_n] \subset S$ que contiene a varios elementos $s_i \in S$.

También podemos añadir nuevos elementos a un anillo R de manera abstracta, es decir, sin tener previamente otro anillo mayor. El propio anillo de polinomios $R[x]$ consiste en añadirle un nuevo elemento x a R de manera libre. Para añadir a R elementos que satisfagan ciertas ecuaciones polinómicas necesitaremos trabajar con cocientes.

A diferencia de otras estructuras algebraicas, no es posible definir el cociente de un anillo por un subanillo. El tipo de subconjunto adecuado para definir cocientes son los ideales.

Recordemos que un **ideal** $I \subset R$ de un anillo R es un subconjunto cerrado para la suma y para el producto por escalares de R que contiene al 0. En particular, si $a_1, \ldots, a_n \in I$ y $r_1, \ldots, r_n \in R$ entonces la **combinación lineal** $r_1 a_1 + \cdots + r_n a_n \in I$. Tanto el total $R \subset R$ como el trivial $\{0\} \subset R$ son ideales. Los cuerpo se caracterizan como los anillos que poseen exactamente dos ideales (necesariamente el total y el trivial). En general, el único ideal que contiene al 1 (o a cualquier otra unidad) es el total. El **núcleo** de un homomorfismo $f\colon R \to S$ es un ideal

$$\ker f = \{a \in R \mid f(a) = 0\}.$$

Este ideal posee la particularidad de que f es inyectivo si y solo si $\ker f = \{0\}$.

El **ideal generado por** un conjunto finto de elementos $a_1, \ldots, a_n \in R$ está formado por todas las combinaciones lineales de los generadores con coeficientes en el anillo:

$$(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n \mid r_1, \ldots, r_n \in R\} \subset R.$$

Este es el menor ideal que contiene a los elementos $a_1, \ldots, a_n \in R$. Es decir, si $I \subset R$ es un ideal y $a_1, \ldots, a_n \in I$ entonces $(a_1, \ldots, a_n) \subset I$.

Un **ideal principal** es uno que está generado por un único elemento $(a) = \{ra \mid r \in R\}$ y que por tanto está formado por sus múltiplos. En $\mathbb{Z}$, el ideal de los números pares es (2).

Dado un anillo y un ideal $I \subset R$, la **clase** de $a \in R$ **módulo** I es el subconjunto

$$a + I = \{a + b \mid b \in I\} \subset R.$$

Estas clases de equivalencia conforman una partición de R denominada anillo **cociente** R/I,

$$R/I = \{a + I \mid a \in R\}.$$

Sabemos que $a + I = b + I$ si y solo si $a - b \in I$. En particular $a + I = 0 + I$ si y solo si $a \in I$. El anillo conciente es un anillo con la suma

$$(a + I) + (b + I) = (a + b) + I$$

y el producto

$$(a + I)(b + I) = (ab) + I.$$

Su cero es $0 + I$ y su uno es $1 + I$. Esto hace que la **proyección natural** $p\colon R \twoheadrightarrow R/I$, $p(a) = a + I$, sea un homomorfismo.

Cuando el ideal I se sobreentiende, sus clases de equivalencia se denotan simplemente

$$a + I = \bar{a} = [a].$$

Dado un polinomio $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$, consideramos el anillo $S = R[x]/(p(x))$. Por abuso de notación, la clase de una constante $a \in R$ en S se denotará igual, $a \in S$, no $\bar{a}$. En este nuevo anillo $\bar{x} \in S$ es una raíz de $p(x)$ puesto que

$$p(\bar{x}) = a_n \bar{x}^n + \cdots + a_1 \bar{x} + a_0 = \overline{p(x)} = \bar{0} \in S.$$

Este anillo posee en ciertos casos una descripción similar a la de los números complejos. Para demostrarlo usaremos el siguiente resultado que asegura que en $R[x]$ siempre podemos dividir por un polinomio mónico del modo habitual.

Lemma 1.1.2.4. *Dado un polinomio* ***mónico*** $p(x) = x^n + \cdots + a_1 x + a_0 \in R[x]$ *y otro polinomio cualquiera* $f(x) \in R[x]$*, existen dos únicos polinomios* $c(x), r(x) \in R[x]$ *tales que* $r(x)$ *tiene grado* $< n$ *y* $f = c \cdot p + r$*.*

Demostración. Sea $f_0 = f$. Si grado $f_0 < n$ entonces podemos tomar $c = 0$ y $r = f_0$. Veamos ahora cómo proceder si grado $f_0 \geq n$. En este caso existen polinomios $c_1, f_1 \in R[x]$ tales que grado $f_1 <$ grado f_0 y $f_0 = c_1 \cdot p + f_1$. En efecto, si

$f_0 = b_m x^m + \cdots$ tiene grado $m \geq n$ podemos tomar $c_1(x) = b_m x^{m-n}$, que tiene sentido pues estamos suponiendo que $m \geq n$. Si el grado de f_1 sigue siendo $\geq n$, podemos aplicar el mismo razonamiento a f_1 obteniendo así polinomios $c_2, f_2 \in R[x]$ tales que grado $f_2 <$ grado f_1 y $f_1 = c_2 \cdot p + f_2$. Podemos continuar

$$\begin{aligned} f_0 &= c_1 \cdot p + f_1, \\ &\vdots \\ f_{i-1} &= c_i \cdot p + f_i, \end{aligned}$$

hasta que grado $f_i < n$. De este modo

$$f = (c_1 + \cdots + c_i) \cdot p + f_i$$

y podemos tomar $c = c_1 + \cdots + c_i$ y $r = f_i$. Hemos probado la existencia.

Veamos la unicidad de r. Si $f = c \cdot p + r = c' \cdot p + r'$ en las condiciones del enunciado, tenemos entonces que $r - r' = (c' - c) \cdot p$. Por un lado $r - r'$ tiene grado $< n$. Supongamos por reducción al absurdo que $c' \neq c$. Entonces $c' - c = e_k x^k + \cdots$ para cierto $k \geq 0$ y $e_k \in R$ no nulo. Esto implica que $(c' - c) \cdot p = e_k x^{k+n} + \cdots$ y por tanto tendría grado $\geq n$. Hemos llegado a una contradicción, así que $c = c'$, luego también $r = r'$. □

Corolario 1.1.2.5. *Dado un polinomio mónico $p(x) = x^n + \cdots + a_1 x + a_0 \in R[x]$ de grado n, todo elemento de $R[x]/(p)$ posee un único representante de grado $< n$.*

Demostración. En efecto, dado $[barf] \in R[x]/(p)$, $r \in R[x]$ es un representante de $[barf]$ si y solo si $barf - r \in (p)$, lo que equivale a la existencia de $c \in R[x]$ tal que $barf - r = c \cdot p$, es decir, $barf = c \cdot p + r$. Este resultado se deduce por tanto del lema anterior. □

Observación 1.1.2.6. El corolario anterior nos dice que, bajo sus condiciones, todo elemento de $R[x]/(p)$ se puede escribir de manera única como

$$b_{n-1}\bar{x}^{n-1} + \cdots + b_1\bar{x} + b_0,$$

donde $b_0, \ldots, b_{n-1} \in R$. La suma de estos representantes se hace coeficiente a coeficiente, como en $\mathbb{C}$. El producto es más complejo y depende de $p(x)$.

En particular, si $n \geq 1$, el homomorfismo $R \hookrightarrow R[x]/(p) \colon r \mapsto \bar{r}$ que envía cada constante a la clase del correspondiente polinomio constante es inyectivo. Por ello, en en estos casos eliminaremos la barra de las clases de los polinomios constantes y las denotaremos simplemente r. De este modo podemos ver R como un subanillo $R \subset R[x]/(p)$. Esto refuerza la idea de que este cociente *añade* el elemento $\bar{x}$ a R.

En adelante, cuando hablemos de añadirle a un anillo R una raíz α de un polinomio $p(x) \in R[x]$ de manera abstracta nos estaremos refiriendo al cociente $R[x]/(p)$ y a $\alpha = \bar{x}$, que como hemos visto es una raíz de $p(x)$ en este anillo. Si p es mónico de grado n, todo elemento de $R[x]/(p)$ se escribe de manera única como $b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$, con $b_0, \ldots, b_{n-1} \in R$.

Ejemplo 1.1.2.7. ($\mathbb{Z}[x]/(x^3+3x+1)$) Todo elemento de este anillo se puede expresar de manera única como $a_2\bar{x}^2 + a_1\bar{x} + a_0$ para ciertos coeficientes $a_0, a_1, a_2 \in \mathbb{Z}$. La suma se calcula sumando coeficientes. El producto es más complejo porque suele ser necesario reducir el grado del representante obtenido. Esto se hace usando que $\bar{x}$ es una raíz del denominador. Concretamente en este caso $\bar{x}^3 + 3\bar{x} + 1 = 0$, luego

$$\begin{aligned}\bar{x}^3 &= -3\bar{x}-1,\\ \bar{x}^4 &= -3\bar{x}^2-\bar{x},\\ \bar{x}^5 &= -3\bar{x}^3-\bar{x}^2\\ &= -3(-3\bar{x}-1)-\bar{x}^2\\ &= -\bar{x}^2+9\bar{x}+3,\\ \bar{x}^6 &= \dots\end{aligned}$$

Usamos esto en el siguiente ejemplo de cálculo,

$$\begin{aligned}(-\bar{x}^2+\bar{x}+2)(\bar{x}+1) &= -\bar{x}^3+3\bar{x}+2\\ &= -(-3\bar{x}-1)+3\bar{x}+2\\ &= 6\bar{x}+3.\end{aligned}$$

Ejemplo 1.1.2.8. $(\mathbb{Z}/(4)[x]/(2x^2-1))$ En este anillo la posible generalización del corolario anterior es totalmente falsa. En efecto, aquí $2=0$ ya que $0=2(2\bar{x}^2-1)=4\bar{x}^2-2=2$ pues $4=0$ en $\mathbb{Z}/4$. Además $\bar{x}^2$ no se puede expresar como la clase de un polinomio de grado <2 porque, si se pudiera, entonces el ideal $(2x^2-1)\subset\mathbb{Z}/(4)[x]$ tendría polinomios mónicos de grado 2, pero no tiene.

Es posible añadir a un anillo de manera abstracta no solo uno sino varios elementos que satisfagan determinadas ecuaciones. Se puede hacer tanto de manera directa como inductiva. Prueba a hacerlo como ejericio.

Frecuentemente necesitaremos construir homomorfismos que partan de anillos cociente. Para facilitar esta tarea disponemos de los dos resultados siguientes.

Proposición 1.1.2.9. *Dado un ideal $I\subset R$ y un homomorfismo $f\colon R\to S$ tal que $I\subset\ker f$, f factoriza de manera única a través de la proyección natural, es decir existe un único homomorfismo $g\colon R/I\to S$ tal que $f=g\circ p$,*

$$f\colon R\overset{p}{\twoheadrightarrow}R/I\overset{g}{\to}S.$$

Demostración. Si $f=g\circ p$ entonces tendríamos

$$f(a)=(g\circ p)(a)=g(p(a))=g(a+I).$$

Definimos la aplicación $g\colon R/I\to S$ como

$$g(a+I)=f(a).$$

Veamos que en efecto está bien definida. La unicidad se seguirá de la primera fórmula.

Si $a+I=a'+I$ entonces $a-a'\in I\subset\ker f$ luego

$$0=f(a-a')=f(a)-f(a').$$

Por tanto

$$g(a+I)=f(a)=f(a')=g(a'+I).$$

Claramente g es un homomorfismo pues se definie como el homomorfismo f en los representantes.

□

Teorema 1.1.2.10. (Primer Teorema de Isomorfía) *Dado un homomorfismo $f\colon R \to S$, existe un único homomorfismo $\bar{f}\colon R/\ker f \to \operatorname{im} f$ tal que f factoriza como $f = i \circ \bar{f} \circ p$, es decir, f encaja en el siguente* ***diagrama conmutativo****,*

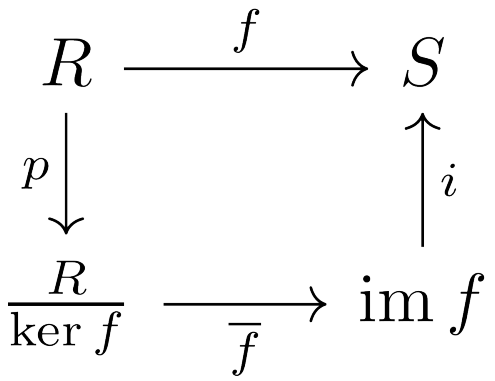

FIGURA 1. Primer teorema de isomorfía

Aquí p es la proyección natural e i es la inclusión. Además $\bar{f}$ es un isomorfismo.

La demostración de este resultado es conocida. Basta recordar que $\bar{f}$ se define como $\bar{f}(\bar{a}) = f(a)$, $a \in R$.

Veamos finalmente que el cuerpo de los números complejos es isomorfo al anillo obtenido al añadirle a $\mathbb{R}$ de manera abstracta una raíz de x^2+1 por el procedimiento anterior.

Corolario 1.1.2.11. $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Demostración. Consideremos el homomorfismo $f\colon \mathbb{R}[x] \to \mathbb{C}$ definido por la inclusión $\mathbb{R} \subset \mathbb{C}$ y tal que $f(x) = i$. Este homomorfismo es sobreyectivo ya que dado $a + ib \in \mathbb{C}$, $f(bx + a) = a + ib$ por tanto $\operatorname{im} f = \mathbb{C}$. Basta ahora ver que $\ker f = (x^2 + 1)$. Como $\mathbb{R}$ es un cuerpo, todo ideal no trivial de $\mathbb{R}[x]$ está generado por cualquiera de sus elementos no nulos de grado mínimo. Por tanto es suficiente comprobar que $x^2 + 1 \in \ker f$ y que $\ker f$ no posee ningún polinomio no trivial de grado < 2. Claramente $f(x^2 + 1) = i^2 + 1 = 0$. Si $bx + a \in \mathbb{R}[x]$ es un polinomio no trivial entonces $f(bx + a) = a + ib$ es un número complejo no trivial, con lo que queda demostrado. □

1.1.3. Cuerpos de fracciones. Recordemos que, dado un anillo R, un **divisor de cero** es un elemento $a \in R$ no nulo, $a \neq 0$, tal que existe otro $b \in R$, $b \neq 0$, de modo que $ab = 0$. Un anillo no trivial R es un **dominio (de integridad)** si no posee divisores de cero.

Dicho de otro modo, R es un dominio cuando dados $a, b \in R$ tales que $ab = 0$ entonces $a = 0$ o $b = 0$. Los dominios poseen la **propiedad cancelativa**, es decir, si $ab = ac$ y $a \neq 0$ entonces $b = c$ ya que esto equivale a $a(b - c) = 0$. Los cuerpos k y los enteros $\mathbb{Z}$ son dominios. Los subanillos de un dominio también son dominios. El anillo $\mathbb{Z}/(6)$ no es un dominio porque aquí $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ pero $\bar{2} \neq \bar{0} \neq \bar{3}$.

Sabemos que si R es un dominio entonces $R[x]$ también y que en dicho caso el grado de un producto es el producto de los grados y las unidades de $R[x]$ son las de R. Por inducción $R[x_1, \ldots, x_n]$ también será un dominio.

Cualquier subanillo de un cuerpo es un dominio. Veamos que, recíprocamente, todo dominio se puede incluir en un cuerpo.

Definición 1.1.3.1. Dado un dominio R, su **cuerpo de fracciones** $Q(R)$ es el cociente del conjunto

$$\left\{ \frac{a}{b} \;\middle|\; a, b \in R,\, b \neq 0 \right\}$$

por la relación de equivalencia

$$\frac{a}{b} \sim \frac{a'}{b'} \Leftrightarrow ab' = a'b$$

dotado de las operaciones

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad+bc}{bd}, \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}. \end{aligned}$$

El ejemplo principal es $Q(\mathbb{Z}) = \mathbb{Q}$.

Proposición 1.1.3.2. *El cuerpo de fracciones $Q(R)$ de un dominio R está bien definido. La aplicación $i\colon R \to Q(R)$, $i(a) = \frac{a}{1}$, es un homomorfismo inyectivo. Todo homomorfismo inyectivo $f\colon R \to k$ donde k es un cuerpo factoriza de manera única a través de i, es decir, existe un único homomorfismo $g\colon Q(R) \to k$ tal que $f = g \circ i$,*

$$f\colon R \xrightarrow{i} Q(R) \xrightarrow{g} k.$$

Demostración. La relación es simétrica y reflexiva porque el producto en R es conmutativo. Veamos la transitividad. Si

$$\frac{a}{b} \sim \frac{a'}{b'} \sim \frac{a''}{b''}$$

entonces

$$\begin{aligned} ab' &= a'b, \\ a'b'' &= a''b'. \end{aligned}$$

En particular,

$$\begin{aligned} (ab'')b' &= (ab')b'' \\ &= (a'b)b'' \\ &= (a'b'')b \\ &= (a''b')b \\ &= (a''b)b'. \end{aligned}$$

Por la propiedad cancelativa de los dominios, $ab'' = a''b$, es decir $\frac{a}{b} \sim \frac{a''}{b''}$. Por tanto el conjunto cociente $Q(R)$ está bien definido. Demostrar que las definiciones de la suma y la multiplicación en $Q(R)$ no dependen de la elección de fracciones representantes es laborioso pero trivial, no es distinto de la construcción clásica de los números racionales. También es fácil probar que los axiomas que definen los anillos se verifican. Obviamente el cero y el uno de $Q(R)$ son $\frac{0}{1}$ y $\frac{1}{1}$, respectivamente.

Por tanto una fracción $\frac{a}{b}$ es nula $\Leftrightarrow a = 0$. Si $\frac{a}{b}$ es no nula entonces es claramente una unidad y $(\frac{a}{b})^{-1} = \frac{b}{a}$, por lo que $Q(R)$ es un cuerpo.

Es inmediato ver que i es un homomorfismo. Es inyectivo porque $a \in \ker f$ si y solo si $\frac{a}{1} = \frac{0}{1}$, lo cual equivale a $a = 0$.

Dado $f\colon R \to k$ como en el enunciado, si existiera una descomposición $f = g \circ i$ entonces tendríamos que

$$f(a) = (g \circ i)(a) = g(i(a)) = g\left(\frac{a}{1}\right).$$

Toda fracción de $Q(R)$ se puede descomponer como

$$\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{1}\left(\frac{b}{1}\right)^{-1},$$

por tanto tendríamos que

$$g\left(\frac{a}{b}\right) = g\left(\frac{a}{1}\left(\frac{b}{1}\right)^{-1}\right) = g\left(\frac{a}{1}\right) g\left(\frac{b}{1}\right)^{-1} = f(a)f(b)^{-1}.$$

Esto demuestra que, caso de existir, g sería único.

Ahora basta definir $g\colon Q(R) \to k$ como $g\left(\frac{a}{b}\right) = f(a)f(b)^{-1}$. Esta definición tiene sentido porque, como $b \neq 0$ y f es inyectivo, $f(b) \neq 0$, y al ser k un cuerpo todo elemento no nulo tiene inverso, luego $f(b)^{-1}$ existe. Con esta definición es un ejercicio comprobar que g es un homomorfismo.

□

Corolario 1.1.3.3. *Dado un homomorfismo inyectivo entre dominios $f\colon R \to S$, existe un único homomorfismo entre sus cuerpos de fracciones $g\colon Q(R) \to Q(S)$ que extiende f, en el sentido de que el siguiente cuadrado es conmutativo*

$$\begin{array}{ccc} R & \xrightarrow{\quad f \quad} & S \\ {\scriptstyle i_R}\downarrow & & \downarrow{\scriptstyle i_S} \\ Q(R) & \xrightarrow[\quad g \quad]{} & Q(S) \end{array}$$

FIGURA 2. Cuerpos de fracciones

es decir, $g \circ i_R = i_S \circ f$, donde i_R e i_S son las inclusiones de R y S en sus cuerpos de fracciones.

Demostración. Basta aplicar la proposición anterior a $i_S \circ f\colon R \to Q(S)$, que es inyectivo por ser composición de inyectivos. El homomorfismo g estará por tanto definido como $g\left(\frac{a}{b}\right) = \frac{g(a)}{g(b)}$. □

Definición 1.1.3.4. Dado un cuerpo k, el **cuerpo de funciones racionales** en una variable se define como $k(x) = Q(k[x])$.

Ejercicio 1.1.3.5. Da dos definiciones del cuerpo de funciones racionales en varias variables $k(x_1, \ldots, x_n)$, una inductiva y otra directa, que sean aparentemente distintas pero isomorfas.

1.1.4. Ideales maximales.

Definición 1.1.4.1. Los ideales distintos del total se denominan **propios**. Un ideal $I \subset R$ es **maximal** si es propio los únicos ideales que lo contienen son I y el total R.

Observación 1.1.4.2. De otro modo, no puede existir ningún ideal J tal que $I \subsetneq J \subsetneq R$. Todo anillo no trivial posee al menos un ideal maximal por el axioma de elección. ¿Cuál es en el caso de los cuerpos?

Recordemos que un ideal $I \subset R$ es **primo** si es propio y dados $a, b \in R$ tales que $ab \in I$ entonces $a \in I$ o $b \in I$.

Si $p \in \mathbb{Z}$ es un primo entonces el ideal $(p) \subset \mathbb{Z}$ es primo ya que si $ab \in (p)$ es porque p divide a ab, luego p ha de dividir a a o a b, es decir $a \in (p)$ o $b \in (p)$.

Sabemos que un ideal $I \subset R$ es primo si y solo si R/I es un dominio. En particular R es un dominio si y solo si el ideal trivial $(0) \subset R$ es primo. Los cuerpos son los anillos cuyo único ideal maximal es (0).

Para dar una caracterización similar de los ideales maximales necesitamos saber cuáles son los ideales de un anillo cociente.

Proposición 1.1.4.3. *Sea $f\colon R \to S$ un homomorfismo.*

- *Si $J \subset S$ es un ideal entonces $f^{-1}(J) \subset R$ también y además $\ker f \subset f^{-1}(J)$.*
- *Si $I \subset R$ es un ideal y f es sobreyectivo entonces $f(I) \subset S$ también es un ideal.*

Demostración. Comenzamos por el primer apartado:

- $0 \in f^{-1}(J)$ porque $f(0) = 0 \in J$.
- Si $a, b \in f^{-1}(J)$ es porque $f(a), f(b) \in J$, luego $f(a+b) = f(a) + f(b) \in J$ y por tanto $a + b \in f^{-1}(J)$.
- Dado $a \in I$ y $r \in R$, $f(ra) = f(r)f(a) \in J$ luego $ra \in f^{-1}(J)$.

Además, como $\{0\} \subset J$, $\ker f = f^{-1}(\{0\}) \subset f^{-1}(J)$.

En el segundo caso:

- $0 = f(0) \in f(I)$ pues $0 \in I$.
- Si $a, b \in I$ entonces $a + b \in I$ luego $f(a) + f(b) = f(a+b) \in f(I)$.
- En el caso anterior también $-a \in I$ luego $-f(a) = f(-a) \in f(I)$.
- Es más, dado $s \in S$, por ser f sobreyectiva $s = f(r)$ para cierto $r \in R$, y como $ra \in I$ entonces $sf(a) = f(r)f(a) = f(ra) \in f(I)$.

□

Teorema 1.1.4.4. (de correspondencia) *Dado un anillo R y un ideal I, si $p\colon R \twoheadrightarrow R/I$ denota la proyección natural tenemos la siguiente biyección*

$$\begin{array}{rcl} \{\textit{ideales de } R \textit{ que contienen a } I\} & \longleftrightarrow & \{\textit{ideales de } R/I\}, \\ I' & \mapsto & p(I'), \\ p^{-1}(J) & \leftarrow & J. \end{array}$$

Demostración. La proyección natural es un homomorfismo sobreyectivo con núcleo I, por tanto las aplicaciones del enunciado están bien definidas por la proposición

anterior. Veamos que una es inversa de la otra. La igualdad $p(p^{-1}(J)) = J$ es cierta por ser p sobreyectiva. En general $I' \subset p^{-1}(p(I'))$. Veamos que la otra inclusión es también cierta si $I \subset I'$. Dado $a \in p^{-1}(p(I'))$, $p(a) \in p(I')$ por tanto existe $b \in I'$ tal que $p(b) = p(a)$. Esto implica que $p(a-b) = p(a) - p(b) = 0$, es decir, $a - b \in I \subset I'$, por tanto $a = b + (a-b) \in I'$. □

Corolario 1.1.4.5. *Un ideal $I \subset R$ es maximal $\Leftrightarrow$ R/I es un cuerpo.*

Demostración. El cociente R/I es un cuerpo si y solo si posee exactamente dos ideales. Esto ocurre si y solo si hay precisamente dos ideales de R que contienen a I. Para que haya más de uno es necesario que $I \subsetneq R$ sea un ideal propio, y que no haya más equivale a que este I sea maximal. □

Corolario 1.1.4.6. *Todo ideal maximal es primo.*

Definición 1.1.4.7. Un **dominio de ideales principales** (también **DIP** o **PID**) es un dominio donde todos los ideales son principales.

Son dominios de ideales principales $\mathbb{Z}$ y $k[x]$ si k es un cuerpo.

Proposición 1.1.4.8. *En un dominio de ideales principales R todos los ideales primos no nulos son maximales.*

Demostración. Supongamos que $(a) \subset (b) \subset R$, con (a) primo y $a \neq 0$. Entonces $a = cb$ para cierto $c \in R$. En particular $cb \in (a)$, que es primo, luego $c \in (a)$ o $b \in (a)$.

Si $b \in (a)$ entonces $(b) \subset (a)$, luego $(a) = (b)$.

Si $c \in (a)$ entonces $c = da$ para cierto $d \in R$, por tanto $a = dab = dba$. Por la propiedad cancelativa $db = 1$, así que b es una unidad, luego $(b) = R$. □

Corolario 1.1.4.9. *En un DIP que no es un cuerpo los ideales maximales son los primos no nulos.*

Ejemplo 1.1.4.10. (Ideales maximales y geometría) Dado un cuerpo k, todo punto $\mathbf{a} = (a_1, \ldots, a_n) \in k^n$ del espacio afín n-dimensional define un ideal maximal de $k[x_1, \ldots, x_n]$,

$$I_{\mathbf{a}} = (x_1 - a_1, \ldots, x_n - a_n).$$

Es en efecto maximal porque es el núcleo del homomorfismo sobreyectivo de evaluación

$$\begin{array}{ccc} k[x_1, \ldots, x_n] & \longrightarrow & k, \\ p(x_1, \ldots, x_n) & \mapsto & p(a_1, \ldots, a_n). \end{array}$$

Por tanto $k[x_1, \ldots, x_n]/I_{\mathbf{a}} \cong k$ es un cuerpo por el primer teorema de isomorfía. El **Teorema de los Ceros de Hilbert** dice que si $k = \mathbb{C}$ o cualquier otro cuerpo algebraicamente cerrado, entonces estos son los únicos ideales maximales de $k[x_1, \ldots, x_n]$, con lo que tendríamos una biyección,

$$\{\text{Ideales maximales de } k[x_1, \ldots, x_n]\} \longleftrightarrow k^n.$$

Como consecuencia de esto y de la caracterización de ideales de un cociente deducimos que si $X \subset k^n$ es el conjunto de soluciones de unas ecuaciones polinómicas, $p_i(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$, $1 \leq i \leq m$,

$$X\colon \begin{cases} p_1(x_1,\dots,x_n)=0,\\ \vdots\\ p_m(x_1,\dots,x_n)=0, \end{cases}$$

entonces tenemos una biyección

$$\{\text{Ideales maximales de } k[x_1,\dots,x_n]/(p_1,\dots,p_m)\} \longleftrightarrow X.$$

El álgebra del anillo cociente $k[x_1,\dots,x_n]/(p_1,\dots,p_m)$ no solo captura el conjunto de puntos de X sino toda su geometría. Por desgracia, otros resultados más precisos al respecto se escapan del alcance de la asignatura.

Ejemplo 1.1.4.11. (Ideales maximales, análisis y topología) Dado un espacio topológico compacto de Hausdorff X, denotamos $\mathcal{C}(X,\mathbb{C})$ al anillo de funciones continuas $X\to\mathbb{C}$. Cualquier punto $x\in X$ define un homomorfismo sobreyectivo de evaluación,

$$\begin{array}{rccc} ev_x\colon \mathcal{C}(X,\mathbb{C}) & \longrightarrow & \mathbb{C},\\ f & \mapsto & f(x), \end{array}$$

cuyo núcleo $\ker ev_x \subset \mathcal{C}(X,\mathbb{C})$ es un ideal maximal por el primer teorema de isomorfía. La **Teoría de Representación de Gelfand** dice que todos los ideales maximales de $\mathcal{C}(X,\mathbb{C})$ son de esta forma, con lo que tenemos una biyección

$$\{\text{Ideales maximales de } \mathcal{C}(X,\mathbb{C})\} \longleftrightarrow X.$$

Esta correspondencia da lugar a una equivalencia de categorías entre los espacios compactos de Hausdorff y las C^*-álgebras conmutativas unitarias, que es una clase de anillos a la que $\mathcal{C}(X,\mathbb{C})$ pertenece. Esto permite estudiar la topología desde el punto de vista del álgebra y del análisis funcional.

1.2. Factorización

La noción clásica de divisibilidad se comporta de manera inesperada en presencia de divisores de cero. Aquí evitaremos estos problemas y estudiaremos la divisibilidad en dominios. Pondremos especial énfasis en el estudio de anillos donde el sea posible generalizar el teorema fundamental de la aritmética. Este teorema, ya conocido para los números enteros, nos dice que todo número no nulo que no sea una unidad factoriza como producto de primos de manera esencialmente única. Este teorema también es conocido para el anillo de polinomios en una variable sobre un cuerpo, en cuyo caso los polinomios irreducibles juegan el papel de los enteros primos. Veremos además cómo este tipo de anillos es de utilidad a la hora de resolver ecuaciones diofánticas.

1.2.1. Divisores.

Definición 1.2.1.1. En un dominio R, decimos que a **divide** a b, o que b es un **múltiplo** de a, y escribimos $a|b$, si $b=aq$ para cierto $q\in R$, que llamaremos **cociente**. Decimos que a es un **divisor propio** de b si además ni a ni q son unidades. Un elemento no trivial de R es **irreducible** si no tiene divisores propios ni es una unidad. Dos elementos a y a' son **asociados** si tanto $a|a'$ como $a'|a$.

Advertencia 1.2.1.2. El cero solo divide al cero, por tanto el cero es el único asociado del cero. Es más, si $a \neq 0$ y $a|b$ el cociente es único, es decir, solo hay un $q \in R$ tal que $b = qa$ pues si $b = q'a$ entonces $qa = q'a$ y por la propiedad cancelativa $q = q'$.

Proposición 1.2.1.3. *En un dominio R:*

- $a|b \Leftrightarrow (a) \supset (b)$.
- $(a) = (a') \Leftrightarrow a$ *y* a' *son asociados* $\Leftrightarrow a' = ua$ *para cierta unidad* u.
- u *es una unidad* $\Leftrightarrow (u) = (1)$.
- a *es un divisor propio de* $b \Leftrightarrow (1) \supsetneq (a) \supsetneq (b)$.

Demostración.

- $(a) \supset (b) \Leftrightarrow (a) \ni b \Leftrightarrow a|b$.
- La primera equivalencia se sigue del apartado anterior. Para la segunda, $\Leftarrow$ es obvio pues también $a = u^{-1}a'$. Veamos $\Rightarrow$. Si a y a' son asociados entonces $a' = qa$ y $a = q'a'$, luego $a = q'qa$. Si $a = 0$ entonces $a' = 0$ y podemos tomar $u = 1$. En caso contrario, por la propiedad cancelativa $1 = q'q$, luego q' y q son unidades y podemos tomar $u = q$.
- $\Rightarrow$ se ha visto antes. $\Leftarrow$ si $(u) = (1)$ entonces existe $r \in R$ tal que $ru = 1$, con lo que u es una unidad.
- Es consecuencia de los tres apartados anteriores.

□

Observación 1.2.1.4. Si $a \in R$ no es nulo ni una unidad, un divisor de a es bien propio, bien asociado, o bien una unidad, pero no puede ser dos de estas cosas a la vez. En particular, si a y a' son irreducibles y $a|a'$ entonces a y a' son asociados. Los divisores de una unidad son las unidades. La primera caracterización de los asociados es especialmente interesante porque demuestra que cualquier propiedad de elementos de R que pueda enunciarse en términos de sus correspondientes ideales principales es también válida para los elementos asociados.

1.2.2. Factorizaciones. En un dominio R, si $a \in R$ es un elemento no trivial que no es una unidad ni tampoco irreducible, entonces podemos descomponerlo como producto de dos divisores propios $a = bc$. Lo mismo podemos hacer con b y con c, y así sucesivamente. Este procedimiento puede acabar en una descomposición de $a = b_1 \cdots b_n$ como producto de elementos irreducibles $b_i \in R$, $1 \leq i \leq n$, pero también podría no acabar nunca.

Definición 1.2.2.1. Decimos que **existen factorizaciones** en un dominio R si el anterior proceso de factorización acaba para todo elemento no nulo que no sea una unidad.

Proposición 1.2.2.2. *En un dominio R existen factorizaciones $\Leftrightarrow$ no existe ninguna sucesión estrictamente creciente de ideales principales* $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$.

Demostración. $\Rightarrow$ En lugar de A $\Rightarrow$ B demostraremos (no A) $\Leftarrow$ (no B). Tomamos pues una sucesión $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$. Podemos suponer que $a_1 \neq 0$ ya que en caso contrario la inclusión estricta $(a_1) \subsetneq (a_2)$ implicaría que $a_2 \neq 0$ y bastaría reindexar. Observa que $(a_n) \subsetneq (1)$ para todo $n \geq 1$, ya que la sucesión es estrictamente creciente y $(1) = R$ es el ideal total. Las inclusiones $(a_n) \subsetneq (a_{n+1}) \subsetneq (1)$ nos dicen entonces que a_n se puede descomponer como producto de divisores propios $a_n = q_{n+1}a_{n+1}$, por tanto el proceso de factorización no termina para

$$\begin{aligned} a_1 &= q_2 a_2 \\ &= q_2 q_3 a_3 \\ &= q_2 q_3 q_4 a_4 \\ &= \cdots , \end{aligned}$$

lo cual es una contradicción.

$\Leftarrow$ Como antes, en lugar de A $\Leftarrow$ B demostraremos (no A) $\Rightarrow$ (no B). Probaremos pues que si no existen factorizaciones entonces podemos encontrar una sucesión $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$. Sea $a_1 \in R$ un elemento no nulo que no sea una unidad para el cual el proceso de factorización no termina. Entonces podemos descomponerlo como producto de divisores propios $a_1 = q_2 a_2$ de modo que alguno de los dos no es irreducible. Como el producto es conmutativo podemos suponer que es a_2 el que no es irreducible. Por tanto este también se puede descomponer como producto de dos divisores propios $a_2 = q_3 a_3$ alguno de los cuales no es irreducible. Una vez más podemos suponer que es a_3 el no irreducible y continuar indefinidamente con el proceso. Por construcción, esto nos da una sucesión creciente $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$ que es estricta porque todas las descomposiciones anteriores son como producto de dos divisores propios. □

La condición de la derecha del enunciado de la proposición anterior se suele denominar **condición de cadena ascendente** para ideales principales. Las condiciones de cadena juegan un papel muy importante en el álgebra moderna. Los anillos que satisfacen la condición de cadena ascendente para ideales cualesquiera se denominan **noetherianos**, por Emmy Noether. Los que cumplen la **condición de cadena descendente** para ideales arbitrarios se llaman **artinianos**, por Emil Artin, padre de Michael, el autor del libro que estamos siguiendo.

Ejemplo 1.2.2.3. (Un dominio sin factorizaciones) No es fácil construir dominios donde no existan factorizaciones. El ejemplo más sencillo es el cociente R/I, donde

$$R = k[x_1, x_2, x_3, \dots]$$

es un anillo de polinomios sobre un cuerpo k en una sucesión infinita de variables $\{x_n\}_{n\geq 1}$ e

$$I = (x_1 - x_2^2, x_2 - x_3^2, x_3 - x_4^2, \dots)$$

es un ideal infinitamente generado que fuerza las relaciones $\bar{x}_n = \bar{x}_{n+1}^2 \in R/I$, $n \geq 1$. En este cociente

$$(\bar{x}_1) \subsetneq (\bar{x}_2) \subsetneq (\bar{x}_3) \subsetneq \cdots .$$

Más concretamente, el proceso $\bar{x}_1 = \bar{x}_2\bar{x}_2 = \bar{x}_2\bar{x}_3\bar{x}_3 = \bar{x}_2\bar{x}_3\bar{x}_4\bar{x}_4 = \cdots$ no termina.

En rigor, es necesario probar que ningún $\bar{x}_i$ es una unidad. Esto es cierto porque de lo contrario existiría algún polinomio $f \in R$ tal que $\bar{x}_i\bar{f} = 1$, o equivalentemente $x_i f - 1 \in I$. Esto es imposible porque los elementos de I, al ser combinaciones lineales de sus generadores, no tienen término independiente.

Definición 1.2.2.4. Un **dominio de factorización única** (también **DFU** o **UFD**) es un dominio donde existen factorizaciones y tal que dos factorizaciones de un mismo elemento coinciden salvo orden y asociados, es decir si

$$b_1 \cdots b_s = c_1 \cdots c_t$$

son productos de irreducibles entonces $s = t$ y existe una permutación $\sigma \in S_s$ de s elementos tal que b_i y $c_{\sigma(i)}$ son asociados, $1 \leq i \leq s$.

Ejemplo 1.2.2.5. (Un dominio con factorizaciones que no son únicas) En $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$,

$$9 = 3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Todo elemento de $\mathbb{Z}[\sqrt{-5}]$ es de la forma

$$z = a + b\sqrt{-5} = a + ib\sqrt{5}$$

donde $a, b \in \mathbb{Z}$. El cuadrado del módulo de tal elemento es

$$|z|^2 = |a + b\sqrt{-5}| = a^2 + 5b^2 \in \mathbb{Z}.$$

Como

$$|z_1 z_2|^2 = |z_1|^2 \cdot |z_2|^2,$$

si $z \in \mathbb{Z}[\sqrt{-5}]$ es una unidad entonces $1 = |z|^2 \cdot |z^{-1}|^2$, así que $|z|^2 \in \mathbb{Z}$ es invertible (y positivo), luego $|z|^2 = 1$. La única posibilidad de que esto ocurra es que $z = \pm 1$, por tanto las unidades de nuestro anillo son $\{\pm 1\}$. Es más, las no unidades tienen módulo al cuadrado > 1, así que si z_1 es un divisor propio de z_2 entonces $|z_1|^2 < |z_2|^2$.

En $\mathbb{Z}[\sqrt{-5}]$ existen factorizaciones. En efecto, si hubiera una cadena $(z_1) \subsetneq (z_2) \subsetneq (z_3) \subsetneq \cdots$ entonces tendríamos que $|z_1|^2 > |z_2|^2 > |z_3|^2 > \cdots \geq 0$, pero esto es imposible, no hay sucesiones infinitas estrictamente decrecientes de enteros no negativos.

Veamos que 3 es irreducible. Si $3 = z_1 z_2$ es una factorización como producto de divisores propios entonces $3^2 = |z_1|^2 |z_2|^2$. No puede ser que $|z_i|^2 = 1$ ya que z_i no es una unidad para ningún $i \in \{1, 2\}$, luego, por el teorema fundamental de la aritmética para números enteros, $|z_1|^2 = |z_2|^2 = 3$, pero no hay ningún elemento en $\mathbb{Z}[\sqrt{-5}]$ que tenga este cuadrado de módulo. Análogamente, $2 \pm \sqrt{-5}$ es irreducible pues si $2 \pm \sqrt{-5} = z_1 z_2$ entonces de nuevo $|2 \pm \sqrt{-5}|^2 = 3^2 = |z_1|^2 |z_2|^2$.

Por último, el 3 no es un asociado de $2 \pm \sqrt{-5}$ porque las únicas unidades de $\mathbb{Z}[\sqrt{-5}]$ son ± 1, luego las dos factorizaciones anteriores de 9 como producto de irreducibles son esencialmente distintas.

Con el objetivo de caracterizar los DFU, introducimos un nuevo tipo de elemento.

Definición 1.2.2.6. Un elemento de un dominio $p \in R$ es **primo** si no es nulo ni una unidad y además si $p|ab$ entonces bien $p|a$ o bien $p|b$.

Observación 1.2.2.7. En términos de ideales, un elemento $p \in R$ no nulo es primo si y solo si $(p) \subset R$ es un ideal primo.

Proposición 1.2.2.8. *En un dominio, todo elemento primo $p \in R$ es irreducible.*

Demostración. El primo no es una unidad porque los ideales primos son distintos del total, $(p) \neq (1)$. Veamos que no tiene divisores propios. Para ello supongamos que $p = ab$ y demostremos que a o b es una unidad. Como $p|ab$, entonces $p|a$ o

$p|b$. Si $p|a$ entonces $a = pq$, luego $p = ab = pqb$. Como los primos no son nulos y estamos en un dominio esto implica que $1 = qb$, por tanto b es una unidad. Si $p|b$ deducimos del mismo modo que a tendría que ser una unidad. □

Ejemplo 1.2.2.9. (Un irreducible que no es primo) Continuando con el ejemplo anterior, el irreducible $3 \in \mathbb{Z}[\sqrt{-5}]$ no es primo porque $3|(2+\sqrt{-5})(2-\sqrt{-5})$ pero $3 \nmid 2 \pm \sqrt{-5}$ porque ambos son irreducibles pero no asociados.

Teorema 1.2.2.10. *Un dominio R es de factorización única $\Leftrightarrow$ existen factorizaciones y todo irreducible es primo.*

Demostración. $\Rightarrow$ Basta ver que los irreducibles son primos. Sea $c \in R$ irreducible. Para ver que es primo, supongamos que $c|ab$. Hay que probar que $c|a$ o $c|b$. Como $c|ab$, entonces $ab = cd$ para cierto $d \in R$. Si $a = 0$ entonces $c|a$ y si $b = 0$, $c|b$. Si a es una unidad, entonces despejando vemos que $c|b$, y si b es una unidad $c|a$. Supongamos en adelante que a y b no son nulos ni unidades. Entonces d no puede ser una unidad, ya que de lo contrario podriamos despejarla y $c = (d^{-1}a)b$ no sería irreducible, pues estaría descompuesto como producto de dos divisores propios. Por tanto a, b y d factorizan como productos de irreducibles,

$$\begin{aligned} a &= a_1 \cdots a_r, \\ b &= b_1 \cdots b_s, \\ d &= d_1 \cdots d_t. \end{aligned}$$

Tenemos pues que

$$a_1 \cdots a_r b_1 \cdots b_s = c d_1 \cdots d_t$$

son dos descomposiciones de un mismo elemento como producto de irreducibles. Por la unicidad, c ha de ser asociado de algún a_i o b_j, por tanto c divide a a o a b.

$\Leftarrow$ Veamos primero que si un primo p divide a un producto de irreducibles $a_1 \cdots a_r$ entonces p es asociado de algún a_i. Procedemos por inducción en r. Para $r = 1$, como $p|a_1$ y ambos elementos son irreducibles, han de ser asociados, según hemos visto anteriormente. Para $r > 1$, como $p|a_1(a_2 \cdots a_r)$, bien $p|a_1$ o bien $p|a_2 \cdots a_r$. En el primer caso, ya tratado, p es asociado de a_1, y en el segundo, por hipótesis de inducción, p es asociado de algún otro a_i.

Consideramos ahora dos productos de irreducibles (primos) que son iguales

$$a_1 \cdots a_r = b_1 \cdots b_s.$$

Supongamos sin pérdida de generalidad que $1 \leq r \leq s$. Procedemos por inducción en r. Si $r = 1$ entonces $s = 1$ puesto que un irreducible no tiene divisores propios. En este caso no hay nada que probar pues $a_1 = b_1$. Sea $r > 1$. Como $a_1|b_1 \cdots b_s$ y a_1 es primo, a_1 es asociado de algún b_i, es decir $b_i = ua_1$ para cierta unidad $u \in R$. Por la propiedad cancelativa

$$a_2 \cdots a_r = u b_1 \cdots \widehat{b_i} \cdots b_s.$$

Observa que b_1 y ub_1 son asociados. Por hipótesis de inducción, las últimas factorizaciones coinciden salvo orden y asociados, por tanto las anteriores también. □

Proposición 1.2.2.11. *En un DFU, un producto de irreducibles $a_1 \cdots a_r$ divide a otro $b_1 \cdots b_s$ si y solo si $r \leq s$ y, salvo reordenamiento, a_i y b_i son asociados $1 \leq i \leq r$.*

Demostración. Como el primer producto divide al segundo, existe $c \in R$ tal que $a_1 \cdots a_r c = b_1 \cdots b_s$. Si c no es una unidad, lo factorizamos como producto de irreducibles $c = c_1 \cdots c_t$,

$$a_1 \cdots a_r c_1 \cdots c_t = b_1 \cdots b_s.$$

Por la unicidad de las factorizaciones, cada a_i es asociado a un b_j distinto, y salvo reordenamiento podemos suponer que son los r primeros. Si c fuera una unidad, la unicidad de las factorizaciones demostraría directamente que $r = s$ y que cada a_i es asociado de un b_j distinto. □

Corolario 1.2.2.12. *Dados dos elementos no nulos de un DFU, $a, b \in R$, existe un **divisor común máximo** $d \in R$, que es un elemento que satisface:*

- *$d|a$ y $d|b$.*
- *si $d'|a$ y $d'|b$ entonces $d'|d$.*

El divisor común máximo es único salvo asociados y se denota $\mathrm{mcd}(a, b)$ *o* $\mathrm{gcd}(a, b)$.

Demostración. Si a o b fuera una unidad, cualquier unidad sería un divisor común máximo puesto los divisores de una unidad son las unidades. En caso contrario, basta factorizar ambos elementos $a = a_1 \cdots a_r$ y $b = b_1 \cdots b_s$ como producto de primos y tomar d como el producto del mayor subconjunto de los factores de a que tienen asociados distintos entre los factores de b. La unicidad salvo asociados se deduce de que si d y d' son divisores comunes máximos de a y b entonces por definición $d|d'$ y $d'|d$. □

Observación 1.2.2.13. Si a o b es una unidad $\mathrm{mcd}(a, b) = 1$. A diferencia de $\mathbb{Z}$ or $k[x]$, k un cuerpo, en un DFU un divisor común máximo no tiene por qué satisfacer una identidad de Bézout, es decir, $\mathrm{mcd}(a, b)$ no tiene por qué estar en el ideal (a, b). Veremos ejemplos más adelante.

Corolario 1.2.2.14. *Dados dos elementos no nulos de un DFU, $a, b \in R$, existe un **múltiplo común mínimo** $m \in R$, que es un elemento que satisface:*

- *$a|m$ y $b|m$.*
- *si $a|m'$ y $b|m'$ entonces $m|m'$.*

El múltiplo común mínimo es único salvo asociados y se denota $\mathrm{mcm}(a, b)$ *o* $\mathrm{lcm}(a, b)$.

Demostración. Si d es un divisor común máximo entonces $m = \frac{ab}{d} = a\frac{b}{d} = \frac{a}{d}b$ es un múltiplo común mínimo. En efecto, la primera propiedad es obvia. Comprobemos la segunda. Si $a|m'$ y $b|m'$ entonces $d|m'$. Es más, $\frac{a}{d}|\frac{m'}{d}$ y $\frac{b}{d}|\frac{m'}{d}$. Como $\frac{a}{d}$ y $\frac{b}{d}$ no tienen factores primos asociados, su múltiplo común mínimo es el producto $\frac{ab}{d^2}$, así que $\frac{ab}{d^2}|\frac{m'}{d}$. Multiplicando por d deducimos que $m = \frac{ab}{d}|m'$. La unicidad salvo asociados se deduce como en el caso del divisor común máximo. □

Lemma 1.2.2.15. *Dada una sucesión creciente de ideales $I_1 \subset I_2 \subset I_3 \subset \cdots$ en un anillo R, su unión $I_\infty = \cup_{n \geq 1} I_n$ es un ideal.*

Demostración. Por un lado, $0 \in I_1 \subset I_\infty$. Por otro, dados $a, b \in I_\infty$ es obvio que $a, b \in I_n$ para cierto $n \geq 1$, por tanto $a + b$, $-a$ y ra, $r \in R$, pertenecen a $I_n \subset I_\infty$. □

Proposición 1.2.2.16. *Todo DIP es un DFU.*

Demostración. Sea R un DIP. Veamos por reducción al absurdo que no puede existir una sucesión estrictamente creciente de ideales principales

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots .$$

Al estar en un DIP, $\cup_{n\geq 1}(a_n) = (b)$ para cierto $b \in R$. Como $b \in \cup_{n\geq 1}(a_n)$ este elemento ha de estar en cierto término de la sucesión, $b \in (a_n)$. Si esto es así $(b) \subset (a_n) \subsetneq (a_{n+1}) \subset (b)$, lo cual es una contradicción.

Veamos ahora que todo irreducible $a \in R$ es primo. Probaremos por reducción al absurdo que el ideal (a) es maximal y por tanto primo. Si (a), que es un ideal propio y no trivial, no fuera maximal podríamos encontrar un ideal I tal que $(a) \subsetneq I \subsetneq R$. Como R es un DIP, $I = (b)$ para cierto $b \in I$. Entonces tenemos que $(a) \subsetneq (b) \subsetneq (1)$. Esto quiere decir que b es un divisor propio de a, lo cual es una contradicción. □

Más adelante veremos ejemplos de DFU que no son DIP.

Proposición 1.2.2.17. *En un DIP, dados $a, b \in R$, cualquier $d \in R$ tal que $(a, b) = (d)$ es un* $\operatorname{mcd}(a, b)$.

Demostración. Como $a, b \in (a, b) = (d)$, d es un divisor común. Si $d'|a$ y $d'|b$ entonces $a, b \in (d')$, luego $(d) = (a, b) \subset (d')$ y por tanto $d'|d$. □

Acabamos de demostrar que en un DIP todo divisor común máximo satisface una **identidad de Bézout**.

Definición 1.2.2.18. Un **dominio euclídeo** es un dominio R equipado con una función

$$\delta \colon R \setminus \{0\} \longrightarrow \{0, 1, 2 \dots\},$$

llamada **función de tamaño** o **euclídea**, tal que dados $D, d \in R$ con $d \neq 0$, denominados **dividendo** y **divisor**, respectivamente, existen $c, r \in R$, **cociente** y **resto**, de modo que

$$D = dc + r$$

y bien $r = 0$ o bien $\delta(r) < \delta(d)$. Esto se denomina **división euclídea** de D por d.

Observación 1.2.2.19. Sabemos que $\mathbb{Z}$ y $k[x]$, con k un cuerpo, son dominios euclídeos con función de tamaño el valor absoluto y el grado, respectivamente. En general, el cociente y el resto no están determinados de manera única por el dividendo y el divisor, por ejemplo

$$13 = 4 \cdot 3 + 1 = 5 \cdot 3 + (-2).$$

Proposición 1.2.2.20. *Un dominio euclídeo R es un DIP. Es más, todo ideal no nulo de R está generado por cualquiera de sus elementos no nulos de tamaño mínimo.*

Demostración. Sea $I \subset R$ un ideal. Si $I = (0)$ ya es principal. Si no, tomamos $a \in I$, $a \neq 0$, de tamaño mínimo. Veamos que $I = (a)$.

Por un lado $(a) \subset I$ pues $a \in I$.

Por otro, dado $b \in I$ realizamos la división euclídea de b por a,

$$b = ca + r.$$

El resto satisface $\delta(r) < \delta(a)$. Además $r = b - ca \in I$, por tanto $r = 0$ y $b = ca \in (a)$.

□

Ejemplo 1.2.2.21. (Los enteros de Gauss) Vamos a ver que $\mathbb{Z}[i]$ con el cuadrado del módulo como función euclídea es un dominio euclídeo. Tomamos $D, d \in \mathbb{Z}[i]$, este último no nulo,

$$\begin{aligned} D &= a + ib, \\ d &= x + iy. \end{aligned}$$

Encontrar un cociente euclídeo se reduce a hallar un múltiplo de d en el interior del círculo de centro D y radio $|d|$. Vamos a ver cómo hacerlo de manera analítica. Consideramos el número complejo

$$\frac{D}{d} = u + iv.$$

Aquí u y v son números reales, de hecho racionales, pero no necesariamente enteros. Aproximamos el anterior número complejo por un entero de Gauss

$$c = u_0 + iv_0 \in \mathbb{Z}[i]$$

de modo que sus partes real e imaginaria estén lo más cerca posible de las del complejo $\frac{D}{d}$,

$$\begin{aligned} |u - u_0| &\leq \tfrac{1}{2}, \\ |v - v_0| &\leq \tfrac{1}{2}. \end{aligned}$$

De este modo

$$\left| \frac{D}{d} - c \right| = \sqrt{(u - u_0)^2 + (v - v_0)^2} \leq \frac{1}{\sqrt{2}}.$$

Veamos que c es el cociente de una división euclídea. El resto sería $r = D - dc$ y su módulo es

$$|r| = |D - dc| = |d| \cdot \left| \frac{D}{d} - c \right| \leq \frac{|d|}{\sqrt{2}} < |d|.$$

Ejemplo 1.2.2.22. (Enteros cuadráticos) Un entero $n \in \mathbb{Z}$ es **libre de cuadrados** no es divisible por el cuadrado de ningún primo, es decir, si entre sus factores primos no podemos encontrar dos asociados. Por ejemplo, $-4 = 2(-2)$ no es libre de cuadrados pero $6 = 2 \cdot 3$ y -1 sí. Los **cuerpos de números cuadráticos** son $\mathbb{Q}[\sqrt{n}] \subset \mathbb{C}$ donde n es un entero libre de cuadrados. Su **anillo de enteros** $R \subset \mathbb{Q}[\sqrt{n}]$ está formado por los elementos que son raíces de un polinomio mónico en $\mathbb{Z}[x]$. Se puede comprobar que $R = \mathbb{Z}[\sqrt{n}]$ si $n \equiv 2, 3 \bmod 4$ y $R = \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ si $n \equiv 1 \bmod 4$. Decimos que R es un **anillo de enteros cuadráticos imaginarios** si $n<0$. Los anillos de enteros cuadráticos imaginarios que son DIPs se obtienen para

$$n = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

De estos, son dominios euclídeos para

$$n = -1, \ -2, \ -3, \ -7, \ -11.$$

En todos estos casos podemos además tomar el cuadrado del módulo como función de tamaño. El resto de anillos de enteros cuadráticos imaginarios no son ni siquiera DFUs. Para $n>0$, obtenemos dominios euclídeos con la 'norma' $N(a+b\sqrt{n}) = a^2 - b^2 n$ para

$$n = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Para $n = 69$, $R = \mathbb{Z}[\frac{1+\sqrt{69}}{2}]$ es también un dominio euclídeo pero no con una función de tamaño distinta de N.

La siguiente aplicación interactiva te permite explorar la posibilidad de realizar divisiones euclídeas respecto del cuadrado del módulo complejo en el anillo de enteros cuadráticos imaginarios $R \subset \mathbb{Q}[\sqrt{-n}]$ para ciertos valores positivos de n. Para $n = 1$ tenemos los enteros de Gauss. Puedes seleccionar los coeficientes del dividendo $D = a + b\sqrt{-n}$ y del divisor $d = x + y\sqrt{-n}$, si $-n \not\equiv 1 \bmod 4$. Si $-n \equiv 1 \bmod 4$, el dividendo y el divisor son de la forma $D = a + b\frac{1+\sqrt{-n}}{2}$ y $d = x + y\frac{1+\sqrt{-n}}{2}$, respectivamente. Los coeficientes del dividendo pueden estar en $[-10, 10]$ y los del divisor en $[-5, 5]$. Aparece un círculo amarillo centrado en D de radio $|d|$. Los puntos verdes son elementos del anillo y los azules son además múltiplos del divisor. Cada punto azul en el *interior* del círculo representa una división euclídea. La aplicación da la lista de todos los pares (c, r) que producen divisiones euclídeas $D = d \cdot c + r$.

1.2.3. Polinomios. En este epígrafe demostraremos que los anillos de polinomios con coeficients en un DFU son también DFUs. En adelante R denotará un DFU y $k = Q(R)$ su cuerpo de fracciones.

Definición 1.2.3.1. Un polinomio no nulo $f = f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ es **primitivo** si el divisor común máximo de sus coeficientes es 1, es decir, si no existe ningún primo $p \in R$ tal que $p|a_i$ para todo $1 \leq i \leq n$.

Los únicos polinomios constantes primitivos son las unidades de R.

Lemma 1.2.3.2. *Dado $f = f(x) = a_n x^n + \cdots + a_1 x + a_0 \in k[x]$ no nulo existe una constante $c \in k$, llamada **contenido**, y un polinomio primitivo $f_0(x) \in R[x]$ tal que*

$$f(x) = c \cdot f_0(x).$$

Además c y $f_0(x)$ son únicos salvo producto por unidades de R. Denotaremos $c = \mathrm{cont}(f)$.

Demostración. Veamos la existencia. Podemos quitar denominadores de los coeficientes de $f(x)$ multiplicando por una constante $d \in R$ no nula,

$$d \cdot f(x) \in R[x].$$

Si e es el divisor común máximo de los coeficientes de $d \cdot f(x)$ vemos que podemos tomar

$$\begin{aligned} f_0 &= \tfrac{d}{e} \cdot f(x), \\ c &= \tfrac{e}{d}. \end{aligned}$$

Probemos ahora la unicidad. Supongamos que $c \cdot f_0(x) = c' \cdot f_0'(x)$ siendo $f_0(x), f_0'(x) \in R[x]$ primitivos. Podemos además suponer sin pérdida de generalidad que $c, c' \in R$, multiplicando por un denominador común si fuera necesario. Como el divisor común máximo de los coeficientesde $f_0(x)$ es 1, el divisor común máximo de los coeficientes de $c \cdot f_0(x)$ es c. Análogamente el divisor común máximo de los coeficientes de $c' \cdot f_0'(x)$ es c'. Por la unicidad del divisor común máximo, c y c' son asociados, es decir $c' = u \cdot c$ donde $u \in R$ es una unidad. Por tanto, por la propiedad cancelativa, $f_0(x) = u \cdot f_0'(x)$. □

Observación 1.2.3.3. Si el contenido de un polinomio $f(x) \in k[x]$ está en R entonces $f(x) \in R[x]$. Recíprocamente, el contenido de un polinomio $f(x) \in R[x]$ es el divisor común máximo de sus coeficientes, en particular $\operatorname{cont}(f) \in R$. Es más, dada una constante $a \in R$ tenemos que $a | f(x)$ si y solo si $a | \operatorname{cont}(f)$. Un polinomio $f(x) \in R[x]$ es primitivo si y solo si $\operatorname{cont}(f) = 1$.

Teorema 1.2.3.4. (Lema de Gauss) *El producto de polinomios primitivos en $R[x]$ es primitivo.*

Demostración. Dado un primo $p \in R$, consideramos el homomorfismo de **reducción módulo** p

$$\phi_p \colon R[x] \longrightarrow (R/(p))[x]$$

definido en las constantes como $\phi_p(a) = \bar{a}$, $a \in R$, tal que $\phi_p(x) = x$. Es decir,

$$\phi_p(a_n x^n + \cdots + a_1 x + a_0) = \bar{a}_n x^n + \cdots + \bar{a}_1 x + \bar{a}_0.$$

El homomorfismo ϕ_p consiste simplemente en reducir los coeficientes módulo (p). En particular $f \in \ker \phi_p$ si y solo si p divide a todos los coeficientes de f. Por tanto $f \in R[x]$ es primitivo si y solo si $\phi_p(f) \neq 0$ para todo $p \in R$ primo. Si $f, g \in R[x]$ son primitivos entonces

$$\phi_p(f \cdot g) = \phi_p(f) \cdot \phi_p(g) \neq 0$$

para todo $p \in R$ primo ya que $(R/(p))[x]$ es un dominio. Es decir, $f \cdot g$ también es primitivo. □

Corolario 1.2.3.5. *Dados $f, g \in k[x]$ tenemos que* $\operatorname{cont}(f \cdot g) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$.

Demostración. Tomamos $f, g \in k[x]$ y los descomponemos

$$\begin{aligned} f &= c \cdot f_0, \\ g &= d \cdot g_0, \end{aligned}$$

con $c, d \in k$ y $f_0, g_0 \in R[x]$ primitivos. Entonces

$$f \cdot g = (c \cdot d) \cdot (f_0 \cdot g_0).$$

Como $f_0 \cdot g_0$ es primitivo por el Lema de Gauss, esta es una descomposición válida del producto $f \cdot g$, así que $c \cdot d$ es su contenido. □

Proposición 1.2.3.6. *Dados $f, g \in R[x]$, si $g | f$ en $k[x]$ y g es primitivo entonces $g | f$ en $R[x]$.*

Demostración. Supongamos que $f = g \cdot q$ en $k[x]$. Como g es primitivo,

$$\text{cont}(f) = \text{cont}(g)\,\text{cont}(q) = \text{cont}(q).$$

Como $f \in R[x]$ su contenido está en R, y como este coindice con el de q, entonces $q \in R[x]$, por lo que $g|f$ en $R[x]$. □

Proposición 1.2.3.7. *Un polinomio $f \in R[x]$ no constante es irreducible en $R[x]$ $\Leftrightarrow$ f es primitivo e irreducible en $k[x]$.*

Demostración. $\Leftarrow$ Supongamos que por reducción al absurdo que f no es irreducible en $R[x]$. Lo descomponemos como producto de divisores propios $f = gh$ en $R[x]$. Si g fuera constante entonces dividiría al contenido de f, que es 1, por tanto g sería una unidad, lo cual entra en contradicción con que sea un divisor propio. Lo mismo ocurriría si h fuera constante. Si g y h no son constantes entonces también son divisores propios de f en $k[x]$, pues no podrían ser unidades, luego f no sería irreducible.

$\Rightarrow$ Si f no fuera primitivo tampoco sería irreducible en $R[x]$ pues su contenido sería un divisor propio. Supongamos por reducción al absurdo que f tiene un divisor propio g en $k[x]$. Aquí ser un divisor propio significa que $0 <$ grado de $g <$ grado de f. Multiplicando por una constante no nula de k si fuera necesario (por el inverso del contenido), podemos suponer que $g \in R[x]$ y es primitivo. Por la proposción anterior g también divide a f en $R[x]$ y por tanto es un divisor propio por cuestión de grados. □

Observación 1.2.3.8. Una constante $a \in R$ es irreducible en $R[x]$ si y solo si lo es en R.

Teorema 1.2.3.9. *$R[x]$ es un DFU.*

Demostración. Primero probamos que existen factorizaciones en $R[x]$. Supongamos por reducción al absurdo que tenemos una sucesión estrictamente creciente de ideales principales (que podemos suponer no nulos) en este anillo,

$$(f_1) \subsetneq (f_2) \subsetneq (f_3) \subsetneq \cdots.$$

Ningún (f_n) puede ser el ideal total porque la sucesión estabilizaría necesariamente a partir de este punto. Por tanto, cada f_{n+1} es un divisor propio de f_n, $n \geq 1$. En particular grado de $0 \leq$ grado de $f_{n+1} \leq$ grado de f_n, es decir, los grados de los generadores forman una sucesion decreciente de enteros no negativos. Esta sucesión de enteros no nulos ha de estabilizar a partir de cierto punto, es decir, ha de existir cierto $n_0 \geq 1$ tal que grado de f_{n+1} = grado de f_n para todo $n \geq n_0$, o equivalentemente $f_n = c_{n+1}f_{n+1}$ para cierto $c_{n+1} \in R$ que no puede ser una unidad ni tampoco nulo. Si llamamos $d_n = \text{cont}(f_n)$ tenemos que $d_n = c_{n+1}d_{n+1}$. Ningún contenido d_n puede ser una unidad porque es divisible por c_{n+1} así que por tanto $d_n = c_{n+1}d_{n+1}$ es una factorización como producto de divisores propios. Sustituyendo reiteradamente vemos que

$$\begin{aligned} d_{n_0} &= c_{n_0+1}d_{n_0+1} \\ &= c_{n_0+1}c_{n_0+2}d_{n_0+2} \\ &= c_{n_0+1}c_{n_0+2}c_{n_0+3}d_{n_0+3} \\ &= \cdots \end{aligned}$$

Por tanto el proceso no termina para d_{n_0}, lo que contradice la existencia de factorizaciones en R.

Veamos que todo elemento irreducible de $R[x]$ es primo. Consideraremos primero el caso en el que nuestro irreducible es un polinomio $f \in R[x]$ no constante. Supongamos que $f|gh$ en $R[x]$. Como f también es irreducible en $k[x]$, que es un DFU, entonces f es primo en $k[x]$ y por tanto $f|g$ o $f|h$ en $k[x]$. Los tres polinomios están en $R[x]$ y al ser f irreducible en este anillo ha de ser primitivo, así que entonces $f|g$ o $f|h$ en $R[x]$.

Supongamos ahora que $a \in R \subset R[x]$ es una constante irreducible y que $a|gh$ en $R[x]$. Esto último equivale adecir que $a|\operatorname{cont}(gh) = \operatorname{cont}(g)\operatorname{cont}(h)$. Como R es un DFU, el irreducible a es primo en R, así que $a|\operatorname{cont}(f)$ o $a|\operatorname{cont}(g)$, es decir, $a|g$ o $a|h$. □

Corolario 1.2.3.10. *$R[x_1, \ldots, x_n]$ es un DFU para todo $n \geq 0$.*

Ejemplo 1.2.3.11. (El anillo $\mathbb{Z}[x]$) Este anillo es un DFU pero no es un DIP. Para comprobarlo basta ver que la identidad de Bézout para el divisor común máximo no siempre se da. Tanto 2 como x son primos en $\mathbb{Z}[x]$ según criterios vistos anteriormente. Como no son asociados, $\operatorname{mcd}(2, x) = 1$, pero $1 \notin (2, x)$ ya que todo elemento de este ideal es de la forma $2g + xh$ para ciertos $g, h \in \mathbb{Z}[x]$, así que su término independiente ha de ser par. Por tanto no hay una identidad de Bézout en este caso. El ideal $(2, x) \subset \mathbb{Z}[x]$ es de hecho un ejemplo de ideal que no es principal.

Tenemos que $R[x] \subset k[x]$. El siguiente resultado nos permite calcular cómo se ven los ideales del segundo dentro del primero.

Proposición 1.2.3.12. *Si $(f) \subset k[x]$ es un ideal no nulo entonces $(f) \cap R[x] = (f_0)$, donde $f = c \cdot f_0$ con $c \in k$ el contenido y $f_0 \in R[x]$ primitivo.*

Demostración. La intersección $(f) \cap R[x]$ es un ideal ya que es la imagen inversa de $(f) \subset k[x]$ a través de la inclusión $R[x] \hookrightarrow k[x]$. Veamos la igualdad de ideales por doble inclusión.

$\supset$ Como $f_0 \in R[x]$ y $f_0 = c^{-1}f \in (f) \subset k[x]$, tenemos que $f_0 \in (f) \cap R[x]$, lo cual demuestra esta inclusión.

$\subset$ Todo elemento $p \in (f)$ es de la forma $p = g \cdot f = (g \cdot c) \cdot f_0$. Si $p \in R[x]$, como $f_0|p$ en $k[x]$ y f_0 es primitivo, $f_0|p$ también en $R[x]$, así que $g \cdot c \in R[x]$ y por tanto $p \in (f_0) \subset R[x]$. □

El siguiente resultado nos demuestra con rigor que las dos posibles maneras de añadirle a R raíces de polinomios irreducibles dan resultados isomorfos.

Teorema 1.2.3.13. *Dado un polinomio irreducible $f \in R[x]$, un cuerpo K tal que $R \subset K$, y una raíz $\alpha \in K$ de f, hay un único isomorfismo $R[x]/(f) \cong R[\alpha] \subset K$ que se comporta sobre R como la identidad y que envía $\bar{x}$ a α.*

Demostración. Por el principio de sustitución, hay un único homomorfismo $g\colon R[x] \to K$ que se restringe a la inclusón $R \subset K$ sobre el dominio de coeficientes y que satisface $g(x) = \alpha$. La imagen de g es $R[\alpha]$ por definición. Por el primer teorema de isomorfía, basta probar que $\ker g = (f) \subset R[x]$.

Recordemos que la inclusión $R \subset K$ se extiende al cuerpo de fracciones k de R, $R \subset k \subset K$. Para probar que $\ker g = (f)$ consideramos la extensión $\bar{g}\colon k[x] \to K$ de g que se define como la inclusión $k \subset K$ sobre el cuerpo de coeficientes y que cumple $\bar{g}(x) = \alpha$. Veamos que $\ker \bar{g} = (f) \subset k[x]$.

El ideal $\ker \bar{g} \subset k[x]$ está formado por todos los polinomios que tienen a α como raíz. Al ser $k[x]$ un dominio euclídeo, $\ker \bar{g} = (\tilde{f})$ donde $\tilde{f} \in k[x]$ es cualquier polinomio no nulo de grado mínimo en este ideal. Realizamos la división euclídea en $k[x]$, $f(x) = c(x)\tilde{f}(x) + r(x)$. Si r no fuera trivial, su grado sería menor que el de $\tilde{f}$, pero $r(x) = f(x) - c(x)\tilde{f}(x)$, por tanto $r(\alpha) = f(\alpha) - c(\alpha)\tilde{f}(\alpha) = 0 - c(\alpha)0 = 0$. Esto es imposible porque $\tilde{f}$ es de grado mínimo. Por tanto $r = 0$ y $f(x) = c(x)\tilde{f}(x)$. El polinomio $c(x)$ ha de ser constante porque f es también irreducible en $k[x]$, así que f y $\tilde{f}$ son asociados, luego generan el mismo ideal, $\ker \bar{g} = (f) \subset k[x]$.

Como $g = \bar{g}|_{R[x]}$, $\ker g = \ker \bar{g} \cap R[x] = (f) \subset R[x]$ en virtud de la proposición anterior, pues $f \in R[x]$, al ser irreducible, es primitivo. Esto concluye la demostración. □

Observación 1.2.3.14. Recuerda que, dado un cuerpo k, un polinomio $f \in k[x]$ de grado ≤ 3 es irreducible si y solo si no tiene raíces en k.

Ejemplo 1.2.3.15. (Los enteros de Gauss como cociente) El polinomio $x^2+1 \in \mathbb{Z}[x]$ es irreducible ya que es primitivo e irreducible en $\mathbb{Q}[x]$ pues su grado es ≤ 3 y no tiene raíces racionales. Por tanto el teorema anterior se aplica a la inclusión $\mathbb{Z} \subset \mathbb{C}$ y a la raíz compleja $i \in \mathbb{C}$ de x^2+1 y obtenemos un isomorfismo con los enteros de Gauss,

$$\begin{array}{ccc} \mathbb{Z}[x]/(x^2+1) & \xrightarrow{\cong} & \mathbb{Z}[i], \\ \bar{x} & \mapsto & i. \end{array}$$

Ejemplo 1.2.3.16. ($\mathbb{Z}[\frac{1}{3}+i]$) Para establecer un isomorfismo entre $\mathbb{Z}[\frac{1}{3}+i] \subset \mathbb{C}$ y un cociente de $\mathbb{Z}[x]$ buscamos un polinomio irreducible con coeficientes enteros que tenga a $\frac{1}{3}+i$ como raíz.

Si denotamos $\alpha = \frac{1}{3}+i$ tenemos que $\alpha - \frac{1}{3} = i$ luego

$$\left(\alpha - \frac{1}{3}\right)^2 = \alpha^2 - \frac{2}{3}\alpha + \frac{1}{9} = -1 = i^2,$$

es decir,

$$\alpha^2 - \frac{2}{3}\alpha + \frac{10}{9} = 0.$$

Dicho de otro modo, α es raíz del polinomio irreducible $x^2 - \frac{2}{3}x + \frac{1}{9} \in \mathbb{Q}[x]$. Este último polinomio se descompone como producto de un racional por un polinomio primitivo con coeficientes enteros del siguiente modo,

$$x^2 - \frac{2}{3}x + \frac{10}{9} = \frac{1}{9}\left(9x^2 - 6x + 10\right).$$

Por tanto $9x^2 - 6x + 10 \in \mathbb{Z}[x]$ es un polinomio irreducible que tiene a $\frac{1}{3}+i$ como raíz, así que, aplicando el teorema anterior a la inclusión $\mathbb{Z} \subset \mathbb{C}$ tenemos un isomorfismo

$$\begin{array}{ccc} \mathbb{Z}[x]/(9x^2-6x+10) & \xrightarrow{\cong} & \mathbb{Z}[\frac{1}{3}+i], \\ \bar{x} & \mapsto & i. \end{array}$$

Corolario 1.2.3.17. *Sea K un cuerpo tal que $R \subset K$ y $\alpha \in K$ la raíz de un polinomio mónico irreducible $f \in R[x]$ de grado n. Entonces todo elemento de $R[\alpha] \subset K$ se escribe de manera única como*

$$b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$$

con $b_0, \ldots, b_{n-1} \in R$.

Demostración. Hemos visto anteriormente que el enunciado es cierto en $R[x]/(f)$ si reemplazamos α por $\bar{x}$, así que el corolario se deduce del isomorfismo del teorema anterior. □

Ejemplo 1.2.3.18. ($\mathbb{Z}[\sqrt{2}]$) El polinomio $x^2 - 2 \in \mathbb{Z}[x]$ es irreducible ya que es primitivo e irreducible en $\mathbb{Q}[x]$ pues su grado es ≤ 3 y no tiene raíces racionales. Así que todo elemento de $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ se puede escribir de manera única como $b_1\sqrt{2} + b_0$, con $b_0, b_1 \in \mathbb{Z}$.

Finalmente veremos un par de condiciones suficientes más avanzadas para la irreducibilidad de un polinomio.

Teorema 1.2.3.19. (Reducción módulo p) *Si $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ es un polinomio primitivo de grado $n > 0$, $p \in R$ es un primo que no divide a_n y la reducción de f módulo p es irreducible en $(R/(p))[x]$, entonces f es irreducible en $R[x]$.*

Demostración. Usaremos el homomorfismo $\phi_p \colon R[x] \to (R/(p))[x]$ de reducción módulo p introducido en la demostración del Lema de Gauss. En general,

$$\text{grado}(\phi_p(f)) \leq \text{grado}(f).$$

La condición sobre a_n equivale a decir que concretamente para el polinomio f del enunciado

$$\text{grado}(\phi_p(f)) = \text{grado}(f).$$

Reduzcamos al absurdo. Si f fuera reducible se descompondría como producto de dos divisores propios $f = gh$. Como f es primitivo, ni g ni h puede ser constante, es decir

$$\text{grado}(g), \text{grado}(h) > 0.$$

Al ser ϕ_p un homomorfismo,

$$\phi_p(f) = \phi_p(g)\phi_p(h).$$

Ninguna de las desigualdades

$$\begin{aligned} \text{grado}(\phi_p(g)) &\leq \text{grado}(g), \\ \text{grado}(\phi_p(h)) &\leq \text{grado}(h), \end{aligned}$$

puede ser estricta ya que de ser así

$$\text{grado}(\phi_p(f)) = \text{grado}(\phi_p(g)) + \text{grado}(\phi_p(h)) < \text{grado}(g) + \text{grado}(h) = \text{grado}(f),$$

pero $\text{grado}(\phi_p(f)) = \text{grado}(f)$. Las dos igualdades de la ecuación anterior son ciertas porque tanto R como $R/(p)$ son dominios, el segundo por ser p primo. Por tanto,

$$\text{grado}(\phi_p(g)), \text{grado}(\phi_p(h)) > 0$$

y tanto $\phi_p(g)$ como $\phi_p(h)$ serían divisores propios de $\phi_p(f)$, que no sería irreducible. □

Teorema 1.2.3.20. (Criterio de Eisenstein) *Si $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ es un polinomio primitivo de grado $n > 0$ y $p \in R$ es un primo tal que:*

- *p no divide a_n,*
- *p divide a $a_{n-1}, \ldots, a_0$,*
- *p^2 no divide a a_0,*

entonces f es irreducible en $R[x]$.

Demostración. Esta demostración transcurre de manera exactamente igual que la anterior hasta la última frase, que no es válida en este caso. A partir de ahí continuamos del siguiente modo. Si $b_0, c_0 \in R$ son los términos independientes de g y h entonces $a_0 = b_0 c_0$. Como $p|a_0$ y p es primo, $p|b_0$ o $p|c_0$, pero no puede dividir a ambos a la vez ya que p^2 no divide a a_0. Esto prueba que bien $\phi_p(g)$ o bien $\phi_p(h)$ tiene término independiente no nulo. Por las condiciones del enunciado, $\phi_p(f) = \bar{a}_n x^n$ con $\bar{a}_n \neq 0$. Al ser $\phi_p(f) = \phi_p(g)\phi_p(h)$ un monomio y $R/(p)$ es un dominio, también $\phi_p(g)$ y $\phi_p(h)$ han de ser monomios. Como uno de ellos tiene término independiente no nulo, entonces ha de tener grado 0, lo que contradice el cálculo al que se llega en la última ecuación de la demostración anterior.

□

1.2.4. Enteros de Gauss. Vamos a estudiar los primos y las factorizaciones en el anillo $\mathbb{Z}[i]$, que es un DFU y un DIP por ser un DE. En nuestros argumentos haremos uso de la conjugación compleja, del módulo y de su cuadrado. Recordemos que el cero es el único elemento de módulo cero y las unidades $\{\pm 1, \pm i\}$ son los elementos de módulo 1.

Proposición 1.2.4.1. *Si $\pi \in \mathbb{Z}[i]$ es primo entonces su conjugado $\bar{\pi}$ también.*

Demostración. Como la conjugación preserva productos, si $\bar{\pi}|ab$ entonces $\pi|\bar{a}\bar{b}$ luego $\pi|\bar{a}$ o $\pi|\bar{b}$, es decir $\bar{\pi}|a$ o $\bar{\pi}|b$. □

Necesitaremos la siguiente observación sobre enteros primos.

Lemma 1.2.4.2. *Todo entero primo $p \in \mathbb{Z}$ satisface una y solo una de las siguientes ecuaciones:*

- *$p \equiv 1$ mod 4.*
- *$p \equiv 3$ mod 4.*
- *$p = \pm 2$.*

Demostración. Si $p \equiv 0 \bmod 4$ entonces p sería un múltiplo de 4, con lo cual no sería primo. Si $p \equiv 2 \bmod 4$ entonces $p = 2 + 4n = 2(1 + 2n)$ para cierto $n \in \mathbb{Z}$, que solo es primo si $1 + 2n$ es invertible en $\mathbb{Z}$, es decir si y solo si $p = \pm 2$. □

Los primos 5, 13, 17, 29, 37, 41, 53, 61… son 1 mod 4, y 3, 7, 11, 19, 23, 31, 43, 47… son 3 mod 4.

Ejercicio 1.2.4.3. Demuestra que hay una cantidad infinita de primos que satisfacen tanto la primera como la segunda ecuación.

Proposición 1.2.4.4. *Si $\pi \in \mathbb{Z}[i]$ es tal que $|\pi|^2 = p \in \mathbb{Z}$ es un entero primo entonces π es primo en los enteros de Gauss y además bien $p = 2$ o bien $p \equiv 1$ mod 4.*

Demostración. Supongamos que π se descompone como $\pi = z_1 z_2$ en $\mathbb{Z}[i]$. Entonces tenemos la ecuación $|z_1|^2|z_2|^2 = |\pi|^2 = p$ de números enteros. Como p es primo en los enteros, necesariamente $|z_i|^2 = 1$ para algún $i \in \{1, 2\}$, es decir, algún z_i tendría que ser una unidad. Esto prueba que el entero de Gauss π es irreducible, luego primo.

Veamos la ecuación en congruencias. Si $\pi = a + ib$ entonces $p = |\pi|^2 = a^2 + b^2$. En $\mathbb{Z}/4$ los únicos elementos que son cuadrados de otros son $0, 1 \in \mathbb{Z}$, por tanto $p = a^2 + b^2$ puede ser 0, 1 o 2 módulo 4. La primera posibilidad queda descartada por el lema anterior y la tercera solo se da cuando $p = 2$. □

De este modo vemos que $1 + i$, $2 + i$, $3 + 2i$, $4 + i$, $5 + 2i$, $6 + i$, $5 + 4i$, $7 + 2i$, $6 + 5i$... son primos en los enteros de Gauss, así como sus conjugados y asociados. En particular $5 = (2 + i)(2 - i)$ es una factorización como producto de primos en $\mathbb{Z}[i]$.

Proposición 1.2.4.5. *Si $p \in \mathbb{Z}$ es un entero primo tal que $p \equiv 3$ mod 4 entonces p también es primo en los enteros de Gauss.*

Demostración. Supongamos por reducción al absurdo que p se descompone como producto de divisores propios $p = z_1 z_2$, entonces tenemos la ecuación $p^2 = |z_1|^2|z_2|^2$ en los enteros. Como ningún z_i es una unidad, necesariamente $|z_1|^2 = |z_2|^2 = p$. Como $p \equiv 3$ mod 4, esto es imposible por la proposición anterior. □

Proposición 1.2.4.6. *Salvo asociados, $1 + i \in \mathbb{Z}[i]$ es el único primo cuyo módulo al cuadrado es 2.*

Demostración. Si $\pi = a + ib$ y $2 = |\pi|^2 = a^2 + b^2$ es fácil observar que $a^2 = b^2 = 1$, es decir $a = \pm 1 = b$. Esto nos da

$$\begin{aligned} 1 + i, & \\ 1 - i &= (-i)(1 + i), \\ -1 + i &= i(1 + i), \\ -1 - i &= (-1)(1 + i). \end{aligned}$$

□

Observación 1.2.4.7. La factorización del 2 como producto de primos en $\mathbb{Z}[i]$ es $2 = (1 + i)(1 - i)$. Los dos primos que aparecen en esta factorización son asociados.

Veamos que para el resto de enteros primos $p \equiv 1$ mod 4 también hay primos en los enteros de Gauss que lo tienen como móldulo al cuadrado y que son de hecho los factores primos de p en $\mathbb{Z}[i]$. Para ello necesitamos resultados técnicos sobre enteros primos.

Lemma 1.2.4.8. *Todo entero primo $p \in \mathbb{Z}$ no negativo satisface la ecuación $(p - 1)! \equiv -1$ mod p.*

Demostración. El resultado es obvio para $p = 2$. Supongamos que $p > 2$. Observemos la definición del factorial

$$(p - 1)! = 1 \underbrace{2 \cdots (p - 2)}(p - 1).$$

Como p es primo, $\mathbb{Z}/(p)$ es un cuerpo y todo elemento no nulo es una unidad. Ningún factor de la definición de $(p - 1)!$ es divisible por p, porque es menor. Por tanto todos son unidades módulo p. En $\mathbb{Z}/(p)$ las únicas unidades que son

inversas de sí mismas son ± 1 ya que estas son las únicas raíces del polinomio $x^2 - 1 = (x-1)(x+1)$. El primer factor de $(p-1)!$ es 1 y el último es $p-1 \equiv -1 \mod p$, por tanto, todos los factores de en medio tienen una inversa diferente, que es otro elemento del mismo producto. Dicho de otro modo, el producto de los $p-3$ factores centrales se puede dividir en $(p-3)/2$ pares de elementos mutuamente inversos módulo p, con lo que este producto es congruente con 1 módulo p, así que $(p-1)! \equiv 1(p-1) \equiv -1 \mod p$. □

Lemma 1.2.4.9. *Si $p \in \mathbb{Z}$ es un entero primo tal que $p \equiv 1$ mod 4 entonces $p|(m^2+1)$ para cierto $m \in \mathbb{Z}$.*

Demostración. Podemos suponer sin pérdida de genralidad que $p \geq 0$. Por el lema anterior, basta ver que $(p-1)!$ es un cuadrado módulo p. Como $p = 4n+1$ entonces

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdots (4n-1) \cdot (4n) \\ &= \underbrace{1 \cdot 2 \cdots (2n-1) \cdot (2n)} \cdot \underbrace{(2n+1) \cdot (2n+2) \cdots (4n-1) \cdot (4n)}.\end{aligned}$$

Para todo $1 \leq i \leq 2n$, en $\mathbb{Z}/(p)$ el i-ésimo factor de la primera mitad es el opuesto por el signo del i-ésimo factor de la segunda mitad empezando por el final ya que ambos suman $4n+1 = p \equiv 0 \mod p$. Por tanto, módulo p,

$$\begin{aligned}(p-1)! &\equiv \underbrace{1 \cdot 2 \cdots (2n-1) \cdot (2n)} \cdot \underbrace{(-2n) \cdot (-2n-1) \cdots (-2) \cdot (-1)} \\ &\equiv (-1)^{2n} \cdot 1^2 \cdot 2^2 \cdots (2n-1)^2 (2n)^2 \\ &= m^2\end{aligned}$$

para $m = (2n)!$. □

En la demostración hemos visto que si $p = 4n+1 \geq 0$ podemos tomar $m = (2n)!$, pero este valor es innecesariamente alto. El siguiente resultado demuestra la existencia de otros más pequeños.

Lemma 1.2.4.10. *En las condiciones del lema anterior, siempre podemos tomar $\sqrt{p-1} \leq m \leq \frac{p}{2}$.*

Demostración. Siempre hay un $0<m<p$ adecuado ya que simplemente se trata de resolver la ecuación $x^2+1 \equiv 0 \mod p$ y el lema anterior demuestra que hay solución. Es más, como la soluciones de esta ecuación no dependen del signo y $-x = p - x \mod p$, podemos escoger $0 < m \leq \frac{p}{2}$. Más aún, si $p|(m^2+1)$ entonces $p \leq m^2 + 1$, luego cualquier solución positiva satisface $m \geq \sqrt{p-1}$. □

Para $p = 13 = 4 \cdot 3 + 1$, el valor del primer lema sería $m = (2 \cdot 3)! = 720$, pero el segundo lema nos garantiza que podemos tomar $3{,}46 \cdots = \sqrt{13-1} \leq m \leq \frac{13}{2} = 6{,}5$, es decir $m = 4, 5$ o 6. Probando estos tres posibles valores vemos que $m = 5$ es el único que satisface $13|(5^2+1) = 26$.

Proposición 1.2.4.11. *Si $p \in \mathbb{Z}$ es un entero primo tal que $p \equiv 1$ mod 4 entonces p no es primo en los enteros de Gauss.*

Demostración. Sabemos que $p|(m^2+1)$ para cierto $m \in \mathbb{Z}$, es decir $p|(m+i)(m-i)$ pero p no divide a $m \pm i$ ya que no divide a su parte imaginaria. Por tanto p no es primo en $\mathbb{Z}[i]$. □

Teorema 1.2.4.12. *Si $p \in \mathbb{Z}$ es un entero primo tal que $p \equiv 1$ mod 4 entonces, salvo asociados, hay exactamente dos primos en los enteros de Gauss cuyo módulo al cuadrado es p. Además estos dos primos son conjugados $\pi, \bar{\pi} \in \mathbb{Z}[i]$.*

Demostración. Como p no es primo en $\mathbb{Z}[i]$ podemos descomponerlo como producto de dos divisores propios $p = z_1 z_2$. Tenemos la ecuación $p^2 = |z_1|^2 |z_2|^2$ en los enteros. Como ningún z_i es una unidad, necesariamente $|z_1|^2 = |z_2|^2 = p$. Según hemos visto antes estos z_i son primos en $\mathbb{Z}[i]$. Es más $z_1 \bar{z}_1 = |z_1|^2 = p = z_1 z_2$, por tanto $z_2 = \bar{z}_1$.

Llamemos $\pi = z_1 = a + ib$. Veamos que π y $\bar{\pi}$ no son asociados. Los asociados de π son

$$\begin{aligned} a + ib, & \\ (-1)(a + ib) &= -a - ib, \\ i(a + ib) &= -b + ia, \\ (-i)(a + ib) &= b - ia. \end{aligned}$$

Veamos que ninguno de estos enteros de Gauss puede ser $\bar{\pi} = a - ib$. Si fuera el primero tendríamos que $b = 0$, pero entonces $p = |\pi|^2 = a^2$, lo cual es una contradicción. Si fuera el segundo tendríamos que $a = 0$ y llegaríamos a la contradicción $p = |\pi|^2 = b^2$. Si fuera el tercero tendríamos que $a = -b$, con lo que $\pi = a(1 - i)$, que solo es primo si a es una unidad, pero en este caso $p = |\pi|^2 = 2 \not\equiv 1$ mod 4. Análogamiente si fuera el último tendríamos que $a = b$ y $\pi = a(1 + i)$, incurriendo en la misma contradicción que en el caso anterior.

Finalmente, comprobemos no puede haber más que estos primos de Gauss y sus asociados con módulo al cuadrado p. En efecto, si $\pi' \in \mathbb{Z}[i]$ satisficiera $p = |\pi'|^2 = \pi' \bar{\pi}'$ entonces como $\pi' | p = \pi \bar{\pi}$ tendríamos que bien $\pi' | \pi$ o bien $\pi' | \bar{\pi}$, es decir, como estos tres elementos son primos, π' es asociado a π o a $\bar{\pi}$. □

Observación 1.2.4.13. En las condiciones del enunciado anterior, la factorización de p en $\mathbb{Z}[i]$ es $p = \pi \bar{\pi}$. Para $p = 5$ los dos primos de Gauss son $\pi = 2 + i$ y $\bar{\pi} = 2 - i$. Los asociados de π son $2 + i$, $-2 - i$, $-1 + 2i$ y $1 - 2i$. Los asociados de $\bar{\pi}$ son los conjugados de los anteriores, $2 - i$, $-2 + i$, $-1 - 2i$ y $1 + 2i$.

Ejemplo 1.2.4.14. (Factores de $p \equiv 1$ mod 4) Dado un entero primo $p \in \mathbb{Z}$ tal que $p \equiv 1$ mod 4, podemos hallar su factorización como producto de primos $p = \pi \bar{\pi}$ en $\mathbb{Z}[i]$ del siguiente modo. Primero encontramos un $m \in \mathbb{Z}$ tal que $p | (m^2 + 1)$. Hemos visto en una demostración anterior que p no divide a $m \pm i$, pero $\pi | p$ y $p | (m^2 + 1) = (m + i)(m - i)$, por tanto el primo de Gauss π divide a $m + i$ o a su conjugado, y análogamente $\bar{\pi}$. Deducimos que π y $\bar{\pi}$ son $\mathrm{mcd}(p, m + i)$ y $\mathrm{mcd}(p, m - i)$.

Por ejemplo, para $p = 13$ hemos visto que podemos tomar $m = 5$. Calculamos $\mathrm{mcd}(13, 5 + i)$, mediante el algoritmo de Euclides. Como el módulo de 13 es mayor que el de $5 + i$, comenzamos realizando la división euclídea del primero por el segundo,

$$13 = (5 + i) \cdot 3 + (-2 - 3i).$$

Ahora dividimos $5 + i$ por el resto de la anterior división,

$$(5 + i) = (-2 - 3i)(-1 + i) + 0.$$

El resto de esta división es 0. El divisor común máximo es el último resto no nulo,

$$\pi = -2 - 3i.$$

Hasta el momento hemos conseguido factorizar los primos enteros en $\mathbb{Z}[i]$ y por tanto calcular aquellos primos de Gauss que son factores de un primo entero. Veamos que estos son todos los primos de Gauss posibles y que por tanto hemos dado ya una descripción completa de todos los primos en $\mathbb{Z}[i]$.

Proposición 1.2.4.15. *Todo primo en $\mathbb{Z}[i]$ divide a un primo en $\mathbb{Z}$.*

Demostración. Sea $\pi \in \mathbb{Z}[i]$ un primo. Factorizamos $|\pi|^2 \in \mathbb{Z}$ como producto de primos enteros $|\pi|^2 = p_1 \cdots p_n$. Como $|\pi|^2 = \pi\bar{\pi}$ entonces $\pi | p_1 \cdots p_n$ así que $\pi | p_i$ para cierto $1 \leq i \leq n$. □

Observación 1.2.4.16. Recapitulando, los primos de Gauss son los siguientes, salvo asociados:

- $1 + i$.
- Los primos enteros $p \in \mathbb{Z}$, $p > 0$, tales que $p \equiv 3 \bmod 4$.
- Para cada primo entero $p \in \mathbb{Z}$, $p > 0$, tal que $p \equiv 1 \bmod 4$, dos primos de Gauss conjugados π y $\bar{\pi}$ tales que $p = \pi\bar{\pi}$, cuyo cálculo se ha explicado en un ejemplo anterior.

Hay una cantidad infinita de primos de Gauss tanto del segundo tipo como del tercer tipo. En $\mathbb{Z}[i]$, los asociados de un elemento se obtienen multiplicándolo por las unidades $\{\pm 1, \pm i\}$.

Ejemplo 1.2.4.17. (Factorizar un entero en $\mathbb{Z}[i]$) Para factorizar $n \in \mathbb{Z}$, $n \neq 0, \pm 1$, como producto de primos en $\mathbb{Z}[i]$, primero lo factorizamos como producto de primos en $\mathbb{Z}$, $n = p_1 \cdots p_r$, y luego factorizamos cada $p_i \in \mathbb{Z}$ como producto de primos en $\mathbb{Z}[i]$. Recuerda que si $p_i \equiv 3 \bmod 4$ entonces ya es primo de Gauss, la factorización del 2 como producto de primos de Gauss es $2 = (1+i)(1-i)$, y el caso $p_i \equiv 1 \bmod 4$ se ha tratado más arriba. Por ejemplo,

$$\begin{aligned} n &= 1350 \\ &= 2 \cdot 3^3 \cdot 5^2 \\ &= (1+i) \cdot (1-i) \cdot 3^3 \cdot (2+i)^2 \cdot (2-i)^2. \end{aligned}$$

Definición 1.2.4.18. Diremos que un entero de Gauss $z = a + ib$ no tiene *parte entera* si $a \neq 0 \neq b$ y $\mathrm{mcd}(a, b) = 1$.

Observación 1.2.4.19. Un entero de Gauss no tiene parte entera si y solo no es divisible por ningún entero distinto de ± 1.

Lemma 1.2.4.20. *Sea z un entero de Gauss sin parte entera y π un primo de Gauss tal que $|\pi|^2 = p$ es un entero primo $p \equiv 1$ mod 4. Si $\pi | z$ entonces $\bar{\pi} \nmid z$.*

Demostración. Por reducción al absurdo, si también $\bar{\pi} \mid p$ entonces $\mathrm{mcm}(\pi, \bar{\pi}) | z$. Como π y $\bar{\pi}$ son primos no asociados, $\mathrm{mcm}(\pi, \bar{\pi}) = \pi\bar{\pi} = p$, por tanto $p | z$ y z tendría parte entera. □

Ejemplo 1.2.4.21. (Factorización de enteros de Gauss sin parte entera) Sea $z \in \mathbb{Z}[i]$ sin parte entera. Supongamos que $z = \pi_1 \cdots \pi_r$ es su factorización como producto de primos de Gauss. Como z no tiene parte entera, ningún π_i es un primo entero $p \equiv 3 \bmod 4$, así que $|\pi_i|^2 = 2$, y en dicho caso π_i es asociado de $1 + i$, o bien

$|\pi_i|^2 = p$ es un primo entero $p \equiv 1 \bmod 4$. Es más, en este último caso ni $\bar{\pi}_i$ ni ninguno de sus asociados puede aparecer en la factorización.

Por tanto, para factorizar z en $\mathbb{Z}[i]$ podemos proceder del siguiente modo. Primero, factorizamos $|z|^2$ como producto de potencias de primos enteros positivos,

$$|z|^2 = p_1^{n_1} \cdots p_s^{n_s}.$$

Entonces

$$z = u\pi_1^{n_1} \cdots \pi_s^{n_s}$$

donde:

- Si $p_i = 2$ entonces $\pi_i = 1 + i$.
- Si $p_i \equiv 1 \bmod 4$, entonces $\pi_i | p$. Para calcularlo, factorizamos p_i como producto de primos de Gauss, $p_i = \pi\bar{\pi}$, según el ejemplo anterior y dividimos $\frac{z}{\pi}$ en $\mathbb{C}$. Si $\frac{z}{\pi}$ resulta ser un entero de Gauss entonces $\pi_i = \pi$, y si no $\pi_i = \bar{\pi}$.
- u es una unidad, $u \in \{\pm 1, \pm i\}$, que se determina a posteriori.

Veámoslo en el caso particular $z = 201 - 43i$. En este caso

$$|z|^2 = 201^2 + 43^2 = 42250 = 2 \cdot 5^3 \cdot 13^2.$$

Las factorizaciones de 5 y de 13 en $\mathbb{Z}[i]$ son $3 = (2+i)(2-i)$ y $13 = (3+2i)(3-2i)$, por tanto

$$z = u(1+i)(2 \pm i)^3(3 \pm 2i)^2.$$

Para determinar qué factor del 5 aparece realmente, dividimos z por uno de ellos en $\mathbb{C}$, por ejemplo

$$\begin{array}{rcl} \frac{z}{2+i} & = & \frac{(201-43i)(2-i)}{(2+i)(2-i)} \\ & = & \frac{359}{5} - \frac{287}{5}i. \end{array}$$

Como no es un entero de Gauss, $2 + i \nmid z$, así que $2 - i \mid z$, luego

$$z = u(1+i)(2-i)^3(3 \pm 2i)^2.$$

Ahora, para hallar qué factor del 13 aparece realmente, dividimos z por uno de ellos en $\mathbb{C}$,

$$\begin{array}{rcl} \frac{z}{3-2i} & = & \frac{(201-43i)(3+2i)}{(3-2i)(3+2i)} \\ & = & 23 + 21i. \end{array}$$

Este sí es un entero de Gauss, por tanto $3 - 2i \mid z$ y

$$z = u(1+i)(2-i)^3(3-2i)^2.$$

Para hallar la unidad, calculamos el producto de la derecha

$$(1+i)(2-i)^3(3-2i)^2 = -43 - 201i,$$

así que $u = i$,

$$z = i(1+i)(2+i)^3(3 \pm 2i)^2.$$

La unidad i se puede incorporar a cualquier factor primo, por ejemplo al primero, $i(1+i) = -1 + i$, y en conclusión

$$z = (-1+i)(2+i)^3(3 \pm 2i)^2$$

es una factorización de z como producto de primos de Gauss.

Ejemplo 1.2.4.22. (Factorización en $\mathbb{Z}[i]$) En general, todo entero de Gauss $z = a+ib \in \mathbb{Z}[i]$ se puede descomponer como $z = n \cdot z'$, con $n = \text{mcd}(a, b)$ y $z' \in \mathbb{Z}[i]$ sin parte entera. La factorización de z como producto de primos de Gauss se obtiene multiplicando las correspondientes factorizaciones de n y z', que se realizan según indicamos aquí y aquí.

Por ejemplo, $z = 15+45i = 15(1+3i)$. Por un lado $n = 15 = 3{\cdot}5 = 3{\cdot}(2+i){\cdot}(2-i)$. Por otro lado $z' = 1 + 3i$, $|z'|^2 = 1^2 + 3^2 = 10 = 2 \cdot 5$. Por tanto

$$z' = u(1+i)(2 \pm i).$$

Para saber qué factor de $5 = (2+i) \cdot (2-i)$ divide a z' realizamos la siguiente operación en $\mathbb{C}$,

$$\begin{array}{rcl} \frac{1+3i}{2+i} & = & \frac{(1+3i)(2-i)}{(2+i)(2-i)} \\ & = & 1+i. \end{array}$$

Por tanto

$$z' = u(1+i)(2+i).$$

De hecho, el cálculo anterior nos demuestra que la unidad es $u = 1$, así que

$$z' = (1+i)(2+i),$$

luego

$$\begin{array}{rcl} z & = & n \cdot z' \\ & = & 3 \cdot (2+i) \cdot (2-i) \cdot (1+i) \cdot (2+i) \\ & = & 3 \cdot (2+i)^2 \cdot (2-i) \cdot (1+i). \end{array}$$

El siguiente gráfico nos muestra la distribución de los primos cercanos al origen en los enteros de Gauss.

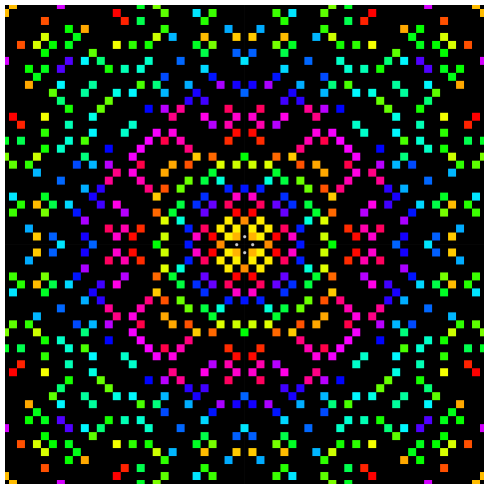

FIGURA 3. Primos de Gauss

Puedes también usar la siguiente aplicación interactiva para explorar la distribución de los primos de Gauss en cuadrados de diferente tamaño centrados en el origen. Los lados del cuadrado tienen tamaño $2n$. Los puntos rojos son los primos de Gauss de módulo al cuadrado 2. En azul están los que son enteros. El resto, en verde.

1.2.5. Ecuaciones diofánticas. A modo de ejemplo, vamos a estudiar aquí un par de ecuaciones diofánticas cuyas soluciones pasan por el estudio de los enteros de Gauss realizado anteriormente.

Al comienzo del tema de anillos nos habíamos planteado como motivación el solucionar la ecuación diofántica

$$x^2 + y^2 = 5.$$

Ahora reemplazaremos el término independiente con un entero positivo > 1 cualquiera.

Teorema 1.2.5.1. *Dado $n \geq 2$, la ecuación diofántica*

$$x^2 + y^2 = n$$

tiene solución si y solo si cualquier primo $p \equiv 3$ mod 4 tiene exponente par en la factorización de n. Además, en dicho caso el número de soluciones es finito.

Demostración. La ecuación planteada equivale a encontrar los enteros de Gauss $x + iy$ tales que $|x + iy|^2 = n$. Si $x + iy = \pi_1 \cdots \pi_n$ es una factorización en $\mathbb{Z}[i]$ entonces $|x + iy|^2 = |\pi_1|^2 \cdots |\pi_n|^2$. Sabemos además, por la clasificación de los primos de Gauss, que $|\pi_i|^2$ puede ser 2, un entero primo $p \equiv 1 \bmod 4$ o p^2 donde $p \equiv 3 \bmod 4$. Esto demuestra la necesidad de la condición del enunciado. También la suficiencia porque, si se cumple, basta tomar $x + iy$ como el producto de:

- Un factor $1 + i$ por cada 2 que aparezca en la factorización de n.
- Si $p \equiv 1 \bmod 4$, un factor π con $|\pi|^2 = p$ por cada factor p de n.
- Si $p \equiv 3 \bmod 4$, un factor p por *cada dos* factores p de n.

El conjunto de todas las soluciones se obtiene permitiendo reemplazar los π del segundo apartado por sus conjugados y tomando los asociados de todas las soluciones particulares así obtenidas. En particular hay un número finito de soluciones. □

Ejemplo 1.2.5.2. ($x^2+y^2 = 1170$) En este caso concreto $1170 = 2\cdot 3^2\cdot 5\cdot 13$. El único primo que vale 3 módulo 4 y que aparece en esta factorización es el propio 3, con exponente par, por lo que la ecuación tiene solución. Una solución se corresponde con el entero de Gauss $x + iy$ obtenido al multiplicar los siguientes factores:

- $1 + i$ por aparecer un 2.
- $2 + i$ por haber un 5 y $2 + 3i$ por haber un 13.
- 3 por el 3^2 que aparece.

Es decir,

$$(1 + i)(2 + i)(2 + 3i)3 = -21 + 27i.$$

Otras soluciones concretas se obtienen permitiendo reemplazar los factores del segundo apartado por sus conjugados,

$$\begin{array}{rcl} (1 + i)(2 - i)(2 + 3i)3 & = & 9 + 33i, \\ (1 + i)(2 + i)(2 - 3i)3 & = & 33 + 9i, \\ (1 + i)(2 - i)(2 - 3i)3 & = & 27 - 21i. \end{array}$$

El conjunto de todas las soluciones $x+iy$ son las cuatro anteriores y sus asociados, 16 en total:

$$\begin{array}{rrrr} -21 + 27i, & 9 + 33i, & 33 + 9i, & 27 - 21i, \\ -27 - 21i, & -33 + 9i, & -9 + 33i, & 21 + 27i, \\ 21 - 27i, & -9 - 33i, & -33 - 9i, & -27 + 21i, \\ 27 + 21i, & 33 - 9i, & 9 - 33i, & -21 - 27i. \end{array}$$

La otra ecuación diofántica que vamos a considerar en este epígrafe es la **ecuación de Pitágoras**

$$x^2 + y^2 = z^2.$$

Sus soluciones positivas $x, y, z > 0$ se denominan **ternas pitagóricas** y parametrizan los triángulos rectángulos con lados de medida entera.

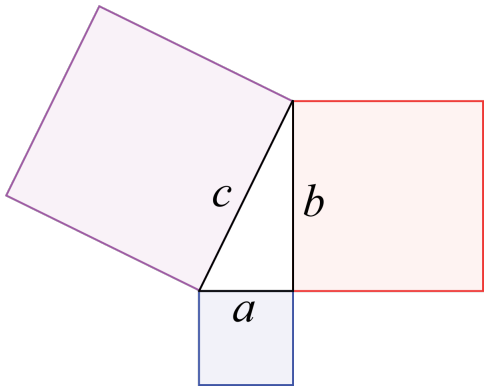

FIGURA 4. Teorema de Pitágoras

Los papeles de x e y en la ecuación de Pitágoras son intercambiables, por lo que (x, y, z) es una solución si y solo si lo es

$$(y, x, z).$$

Los signos de las soluciones son irrelevantes, es decir si (x, y, z) es una solución entonces también lo son

$$(\pm x, \pm y, \pm z).$$

Las soluciones triviales son las de la forma $(x, 0, \pm x)$ o $(0, y, \pm y)$. Por tanto basta estudiar las ternas pitagóricas.

No hay ternas pitagóricas con x e y impares porque en ese caso $x \equiv \pm 1$ e $y \equiv \pm 1$ mod 4, así que $z^2 = x^2 + y^2 \equiv 1 + 1 = 2 \bmod 4$. Esto es imposible porque los únicos cuadrados en $\mathbb{Z}/(4)$ son 0 y 1.

Si (x, y, z) es una terna pitagórica y $d = \mathrm{mcd}(x, y)$ entonces $d^2|x^2$ y $d^2|y^2$ por lo que $d^2|z^2$. Por tanto $d|z$ y

$$\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$$

es otra terna pitagórica con $\mathrm{mcd}(\frac{x}{d}, \frac{y}{d}) = 1$. En definitiva, podemos centrarnos en buscar las ternas pitagóricas (x, y, z) tales $\mathrm{mcd}(x, y) = 1$. Estas se denominan **ternas pitagóricas primitivas**. Las que no son primitivas se obtienen a partir de las primitivas multiplicando por enteros positivos. En una terna pitagórica primitiva x e y no pueden ser ambos pares. A la luz del párrafo anterior, x ha de ser par e y impar, o viceversa, es decir,

$$x \not\equiv y \quad \text{mód } 2.$$

Podemos pues suponer que x es impar e y es par, el resto de ternas pitagóricas primitivas se obtendrán intercambiando la x y la y.

La conexión de la ecuación de Pitágoras con los enteros de Gauss proviene de que esta ecuación equivale a

$$(x + iy)(x - iy) = z^2.$$

Lemma 1.2.5.3. *Dados $x, y \in \mathbb{Z}$ no nulos, tenemos que $x \equiv y$ mod 2 $\Leftrightarrow$ $(1 + i)|(x + iy)$.*

Demostración. $\Rightarrow$ Si $x \equiv y \bmod 2$ entonces x e y son ambos pares o ambos impares. Si son ambos pares entonces $2|(x + iy)$ y ya sabemos que $(1 + i)|2$ con lo que $(1 + i)|(x + iy)$. Si son ambos impares entonces $y \pm x$ es par y tenemos la siguiente ecuación en $\mathbb{Z}[i]$,

$$x + iy = (1 + i)\left(\frac{y + x}{2} + i\frac{y - x}{2}\right).$$

$\Leftarrow$ Si $(1 + i)|(x + iy)$ entonces

$$x + iy = (1 + i)(x' + iy') = (x' - y') + (x' + y')i$$

y por tanto

$$x = x' - y' \equiv x' + y' = y \quad \text{mód } 2.$$

□

En el siguiente lema caracterizamos en términos de los enteros de Gauss la condición sobre x e y que caracteriza las ternas pitagóricas que son primitivas.

Lemma 1.2.5.4. *Dados $x, y \in \mathbb{Z}$ no nulos, tenemos que* $\mathrm{mcd}(x, y) = 1$ *y* $x \not\equiv y$ *mod* $2 \Leftrightarrow \mathrm{mcd}(x + iy, x - iy) = 1$.

Demostración. $\Rightarrow$ Por reducción al absurdo. Si $\pi \in \mathbb{Z}[i]$ es un primo de Gauss tal que $\pi|(x + iy)$ y $\pi|(x - iy)$ entonces

$$\begin{array}{rcl} \pi \mid [(x + iy) + (x - iy)] & = & 2x, \\ \pi \mid [(x + iy) - (x - iy)] & = & 2yi. \end{array}$$

El primo π no puede dividir simultáneamente a x y a y ya que $\mathrm{mcd}(x, y) = 1$, y el divisor común máximo de dos enteros es el mismo calculado en $\mathbb{Z}$ o en $\mathbb{Z}[i]$. De aquí deducimos que $\pi|2$, es decir $\pi = 1+i$ (o un asociado). Por tanto $(1+i)|(x+iy)$, así que por el lema anterior $x \equiv y \bmod 2$, lo cual es una contradicción.

$\Leftarrow$ Cualquier divisor común de x e y divide tanto a $x + iy$ como a $x - iy$, por tanto $\mathrm{mcd}(x, y) = 1$. Además $x \not\equiv y \bmod 2$ ya que en caso contrario, por el lema anterior, $(1+i)|(x+iy)$ y por tanto $(1-i)|(x-iy)$. Como $1+i$ y $1-i$ son asociados, ambos dividirían tanto a $x + iy$ como a $x - iy$, que no podrían ser coprimos. □

Lemma 1.2.5.5. *En un DFU R, las soluciones no nulas de la ecuación $xy = z^2$ tales* $\mathrm{mcd}(x, y) = 1$ *son, salvo asociados, todas de la forma $x = a^2$, $y = b^2$ y $z = ab$ con $a, b \in R$,* $\mathrm{mcd}(a, b) = 1$.

Demostración. Si z fuera una unidad, entonces también lo tendrían que ser z^2, x e y, por tanto, salvo asociados, $x = y = z = 1 = 1^2$. Supongamos ahora que z no es una unidad. Sea $z = p_1 \cdots p_n$ una factorización como producto de primos. Como $xy = z^2 = p_1^2 \cdots p_n^2$, por la unicidad de las factorizaciones en R los factores primos de z^2 se han de repartir entre x e y, salvo asociados. Además, como $\mathrm{mcd}(x, y) = 1$, los dos factores de cada p_i^2 tienen que quedar del mismo lado, por lo que tanto x como y son cuadrados, $x = a^2$ e $y = b^2$, y $z = ab$, de nuevo salvo asociados. Además $\mathrm{mcd}(a, b) = 1$ porque $1 = \mathrm{mcd}(x, y) = \mathrm{mcd}(a, b)^2$. □

Teorema 1.2.5.6. *Las ternas pitagóricas primitivas con segunda coordenada par son las de la forma $(a^2 - b^2, 2ab, a^2 + b^2)$ con $a, b \in \mathbb{Z}$, $a > b > 0$,* $\mathrm{mcd}(a, b) = 1$, *$a \not\equiv b$ mod 2.*

Demostración. La ecuación de Pitágoras, vista en $\mathbb{Z}[i]$, es

$$(x + iy)(x - iy) = z^2.$$

Según hemos visto mas arriba, la condición de que una terna pitagórica sea primitiva equivale a $\mathrm{mcd}(x+iy, x-iy) = 1$. Por el lema anterior, tanto $x+iy$ como $x - iy$ son cuadrados, o asociados de cuadrados, necesariamente conjugados. Es decir, $x + iy = u(a + ib)^2$ para cierto $u = 1, -1, i, -i$. Esto da lugar a las siguientes posibilidades:

$$(x, y) = \begin{cases} (a^2 - b^2, 2ab), \\ (b^2 - a^2, -2ab), \\ (-2ab, a^2 - b^2), \\ (2ab, b^2 - a^2). \end{cases}$$

Las dos últimas no dan lugar al tipo de terna pitagórica primitiva que estamos considerando, pues x sería par. La primera sí, siempre que $a > b > 0$, pues $x, y > 0$. También si $ a < b < 0$, pero por este camino llegaríamos a las mismas ternas. La segunda posibilidad también da lugar a las mismas ternas que la primera. Así que podemos suponer que $x+iy = (a+ib)^2$ con $a > b > 0$ y por tanto $x-iy = (a-ib)^2$.

De nuevo por el lema anterior,

$$z = u(a + ib)(a - ib) = u(a^2 + b^2)$$

para cierta unidad $u \in \{\pm 1, \pm i\}$. Como la ecuación $(x + iy)(x - iy) = z^2$ ha de satisfacerse, la unidad ha de ser tal que $u^2 = 1$, con lo que $u = \pm 1$. El caso $u = -1$ lo excluimos ya que entonces $z = -(a^2 + b^2) < 0$, por tanto $z = a^2 + b^2$. Además, una vez más por el lema anterior, $\mathrm{mcd}(a + ib, a - ib) = 1$, es decir $\mathrm{mcd}(a, b) = 1$ y $a \not\equiv b \bmod 2$, usando el lema de más arriba. Esto reduce todas las posibilidades a las que aparecen en el enunciado del teorema. Veamos que todas ellas son en efecto ternas pitagóricas primitivas.

Claramente, las ternas del enunciado resuelven la ecuación de Pitágoras, es decir,

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

Las tres coordenadas son positivas, pues $a > b > 0$. La segunda coordenada es claramente par. Solo queda comprobar que las dos primeras son coprimas. Para ello, demostraremos que la primera no es divisible por 2 ni por ningún factor primo de a o de b. Como $n \equiv n^2 \bmod 2$ para todo $n \in \mathbb{Z}$, $a^2 - b^2 \equiv a - b \not\equiv 0 \bmod 2$, pues $a \not\equiv b \bmod 2$, así que $a^2 - b^2$ es impar. Sea $p \in \mathbb{Z}$ un primo. Si $p \mid a$ entonces $p \mid a^2$. Si fuera cierto que $p \mid (a^2 - b^2)$ entonces tendriamos que $p \mid b^2$ y por tanto $p \mid b$. Esto contradeciría que $\mathrm{mcd}(a, b) = 1$, luego en realidad $p \nmid (a^2 - b^2)$. Análogamente se prueba que si $p \mid b$ entonces $p \nmid (a^2 - b^2)$. Esto concluye la demostración. □

El siguiente gráfico muestra los pares (x, y) que forman parte de una terna pitagórica cualquiera con $x, y \leq 4500$.

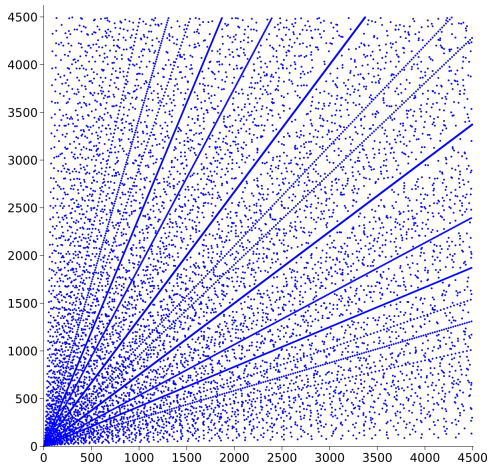

FIGURA 5. Ternas pitagóricas

La siguiente aplicación muestra los pares (x, y) que forman parte de una terna pitagórica primitiva con x impar y $x, y \leq n$, donde n puede ser cualquier múltiplo de 10 comprendido entre 10 y 3000.

Parte 2. Módulos

¿Cómo es el álgebra lineal que resulta al reemplazar el papel de los cuerpos por anillos más generales? El objeto de estudio de esta álgebra lineal generalizada son los módulos. Un módulo M es a un anillo R lo que un espacio vectorial es a un cuerpo. Es decir, el módulo M está dotado de las siguientes operaciones:

- Suma.
- Resta.
- Producto por escalares de R.

Estas operaciones deben satisfacer las propiedades habituales. Además el módulo ha de contener el siguiente elemento:

- Cero 0.

Tanto este $0 \in M$ como el $1 \in R$ han de satisfacer las propiedades habituales con respecto a la suma y la multiplicación.

Los módulos sobre el anillo $\mathbb{Z}$ son simplemente los grupos abelianos. Los espacios vectoriales sobre un cuerpo cualquiera están clasificados por su dimensión. Es decir, dos espacios vectoriales son isomorfos si y solo si tienen la misma dimensión. En este tema estudiaremos fundamentalmente la clasificación de los módulos finitamente generados sobre un dominio de ideales principales. En particular la clasificación de los grupos abelianos finitamente generados. Aplicaremos estos resultados a la resolución de sistemas de ecuaciones lineales diofánticas y al estudio de un tema de álgebra lineal clásica: los endomorfismos de espacios vectoriales de dimensión finita.

Parte 3. Cuerpos

¿Sabías que es imposible construir un hepágono regular con una regla y un compás? ¿Sabías que también es imposible construir de este modo un cuadrado con la misma área que un círculo dado? Este último problema se conoce como la **cuadratura del círculo**. Fue planteado en la antigüedad y permaneció abierto hasta finales del siglo XIX.

Seguro que sabes que la única raíz de un polinomio de grado 1, $ax + b$, es

$$x = -\frac{b}{a}.$$

También sabes que las raíces de uno de grado 2, $ax^2 + bx + c$, son

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Es menos conocido que las raíces de un polinomio de grado 3, $ax^3 + bx^2 + cx + d$, son

$$x = \begin{cases} S + T - \frac{b}{3a}, \\ -\frac{S+T}{2} - \frac{b}{3a} + \frac{i\sqrt{3}}{2}(S - T), \\ -\frac{S+T}{2} - \frac{b}{3a} - \frac{i\sqrt{3}}{2}(S - T), \end{cases}$$

donde

$$\begin{aligned} S &= \sqrt[3]{R+\sqrt{Q^3+R^2}}, \\ T &= \sqrt[3]{R-\sqrt{Q^3+R^2}}, \\ Q &= \tfrac{3ac-b^2}{9a^2}, \\ R &= \tfrac{9abc-27a^2d-2b^3}{54a^3}. \end{aligned}$$

De aquí surge por tanto la siguiente cuestión natural: ¿Es posible expresar las raíces de un polinomio de cualquier grado a partir de sus coeficientes mediante sumas, multiplicaciones y raíces iteradas? Esto se denomina resolver una ecuación polinómica por **radicales**. Esta importante pregunta es también de origen antiguo y permaneció abierta hasta el siglo XIX, cuando fue resuelta por Galois. La respuesta es sencilla, aunque llegar a ella no es fácil: hasta grado 4 sí, de grado 5 en adelante, en general, no. Un ejemplo de polinomio de grado 5 cuyas raíces no se pueden hallar por radicales es el siguiente, a pesar de su aparente sencillez,

$$x^5 - 16x + 2.$$

A lo largo de este capítulo estudiaremos las matemáticas necesarias para resolver estas y otras cuestiones relacionadas.

3.1. Extensiones

3.1.1. Extensiones de cuerpos.

Definición 3.1.1.1. Una **extensión (de cuerpos)**

$$F \subset K$$

es un par formado por un cuerpo K y un subanillo F que también es un cuerpo. Decimos en este caso que K es una extensión de F. Observa que K es un F-espacio vectorial con la suma y el producto por escalares de F. La extensión es **finita** si $\dim_F K < \infty$, en dicho caso definimos el **grado** de la extensión como

$$[K : F] = \dim_F K.$$

Observación 3.1.1.2. El grado de una extensión $F \subset K$ es $[K : F] \geq 1$. No hay extensiones de grado 0 ya que todo cuerpo $K \neq 0$.

Ejemplo 3.1.1.3. (Ejemplos de extensiones)

- $\mathbb{R} \subset \mathbb{C}$ es finita de grado $[\mathbb{C}, \mathbb{R}] = 2$, ya que $\{1, i\} \subset \mathbb{C}$ es una base como $\mathbb{R}$-espacio vectorial.
- $\mathbb{Q} \subset \mathbb{R}$ no es finita porque cualquier $\mathbb{Q}$-espacio vectorial de dimensión finita es numerable, pero $\mathbb{R}$ no lo es.
- Todo cuerpo F posee la **extensión trivial** $F \subset F$, que es la única de grado 1, el resto tienen grado > 1. En efecto, $\dim_F F = 1$ así que, como $F \subset K$, $[K : F] = \dim_F K \geq 1$ dándose la igualdad si y solo si $F = K$.
- $F \subset F(x)$ tampoco es finita.
- $F \subset F[x]/(p(x))$, donde $p(x) \in F[x]$ es un polinomio irreducible. En efecto, por ser $F[x]$ un DFU tenemos que $p(x) \in F[x]$ es primo, y por ser $F[x]$ un dominio de ideales principales tenemos que el ideal primo $(p(x)) \subset F[x]$,

al ser no trivial, es maximal, por tanto $F[x]/(p(x))$ es un cuerpo. Sabemos además que

$$[F[x]/(p(x)) : F] = \text{grado } p(x).$$

Definición 3.1.1.4. Dadas dos extensiones $F \subset K$ y $F \subset L$ de un mismo cuerpo F, un **homomorfismo** de extensiones $f\colon K \to L$ es un homomorfismo de anillos que deja fijo a F, es decir, que satisface $f(\alpha) = \alpha$ para todo $\alpha \in F$. Un **endomorfismo** de una extensión $F \subset K$ un homomorfismo de extensiones $f\colon K \to K$. Un **isomorfismo** de extensiones es un homomorfismo biyectivo. Un **automorfismo** de una extensión $F \subset K$ es un endomorfismo biyectivo.

La conjugación $\mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$, es un homomorfismo de extensiones de $\mathbb{R}$ ya que $x = \bar{x}$ para todo $x \in \mathbb{R}$.

Observación 3.1.1.5. La identidad es un homomorfismo de extensiones y la composición de homomorfismos de extensiones es también un homomorfismo de extensiones. Lo mismo ocurre con isomorfismos y automorfismos. Además, la aplicación inversa de un isomorfismo de extensiones es otro isomorfismo de extensiones, e igual para los automorfismos. Los homorfismos de cuerpos son inyectivos, así que los homomorfismos de extensiones también.

Proposición 3.1.1.6. *Un homorfismo $f\colon K \to L$ de extensiones de F es también un homomorfismo de F-espacios vectoriales.*

Demostración. Como f es un homomorfismo de anillos, preserva sumas. Dado $\alpha \in F \subset K$ y $x \in K$, por ser f un homomorfismo de anillos, $f(\alpha x) = f(\alpha)f(x)$. Como f es un homomorfismo de extensiones de F, $f(\alpha) = \alpha$. Por tanto $f(\alpha x) = \alpha f(x)$, es decir, f preserva el producto por escalares de F. □

Corolario 3.1.1.7. *Si $f\colon K \to L$ es un isomorfismo de extensiones de F entonces $[K : F] \cong [L : F]$.*

Más adelante veremos ejemplos de extensions no isomorfas del mismo grado.

Corolario 3.1.1.8. *Todo endomorfismo $f\colon K \to K$ de una extensión finita $F \subset K$ es un automorfismo.*

Demostración. Como f es un homomorfismo inyectivo de F-espacios vectoriales y su partida y su llegada poseen la misma dimensión, ha de ser un isomorfismo. □

Proposición 3.1.1.9. *Dadas dos extensiones $\mathbb{Q} \subset K$ y $\mathbb{Q} \subset L$ de $\mathbb{Q}$, cualquier homomorfismo de anillos $f\colon K \to L$ es un homomorfismo de extensiones.*

Demostración. Por ser f un homomorfismo de anillos, $f(0) = 0$. Es más, como $f(1) = 1$ y f preserva sumas, es fácil ver que $f(n) = n$ para cualquier $n \in \mathbb{Z}$, $n > 0$. Además f preserva opuestos, luego $f(-n) = -f(n) = -n$. Esto prueba que f deja fijo a $\mathbb{Z}$. Todo racional se puede expresar como $\frac{p}{q} = pq^{-1}$ para $p, q \in \mathbb{Z}$, $q \neq 0$. Los homomorfismos de anillos preservan productos e inversos, así que

$$\begin{aligned} f\left(\tfrac{p}{q}\right) &= f(pq^{-1}) \\ &= f(p)f(q^{-1}) \\ &= f(p)f(q)^{-1} \\ &= pq^{-1} \\ &= \tfrac{p}{q}. \end{aligned}$$

□

Corolario 3.1.1.10. *Dada una extension finita $\mathbb{Q} \subset K$, todo homomorfismo de anillos $f\colon K \to K$ es un automorfismo de la extensión $\mathbb{Q} \subset K$.*

Definición 3.1.1.11. Dada una extensión $F \subset K$, decimos que $\alpha \in K$ es **algebraico** si existe $p(x) \in F[x]$ no nulo tal que $p(\alpha) = 0$. En caso contrario decimos que α es **trascendente**.

Observación 3.1.1.12. Si tenemos dos extensiones sucesivas $F \subset K \subset L$ y $\alpha \in L$ es algebraico sobre F entonces también es algebraico sobre K ya que $F[x] \subset K[x]$. ¡Ojo! El recíproco no es cierto. Todo $\alpha \in F$ es algebraico sobre F ya que es raíz de $x - \alpha \in F[x]$.

El elemento $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, aunque $\sqrt{2} \notin \mathbb{Q}$. Análogamente $i \in \mathbb{C}$ es algebraico sobre $\mathbb{R}$ ya que es raíz de $x^2 + 1 \in \mathbb{R}[x]$, y también sobre $\mathbb{Q}$.

Ejemplo 3.1.1.13. (Existencia de elementos trascendentes en $\mathbb{Q} \subset \mathbb{C}$) Como $\mathbb{Q}$ es numerable, $\mathbb{Q}[x]$ también. Además, todo polinomio tiene una cantidad finita de soluciones en $\mathbb{C}$. Por tanto hay una cantidad numerable de elementos algebraicos para la extensión $\mathbb{Q} \subset \mathbb{C}$. Como $\mathbb{C}$ no es numerable, han de existir elementos trascendentes, de hecho una cantidad no numerable de ellos. Lo mismo se aplica a la extensión $\mathbb{Q} \subset \mathbb{R}$. Dar un ejemplo concreto de número trascendente es sin embargo bastante complicado. Es conocido que π es trascendente sobre $\mathbb{Q}$ pero no es fácil probarlo.

Definición 3.1.1.14. Dada una extensión $F \subset K$ y un elemento algebraico $\alpha \in K$, su **polinomio irreducible** $p(x) \in F[x]$ es el único polinomio mónico irreducible con coeficientes en F que tiene a α como raíz. El **grado** de α sobre F es el de su polinomio irreducible.

Observación 3.1.1.15. La existencia del polinomio irreducible de un elemento algebraico no es obvia y la veremos como consecuencia del siguiente teorema. También es posible probarla usando que $F[x]$ es un DFU. La condición de ser mónico es solo para garantizar su unicidad. Si encontramos un polinomio irreducible en $F[x]$ que tiene a α como raíz, basta dividirlo por su coeficiente líder para convertirlo en mónico.

Teorema 3.1.1.16. *Dada una extensión $F \subset K$ y un elemento algebraico $\alpha \in K$, el polinomio irreducible de α es el generador mónico del núcleo del homomorfismo $f\colon F[x] \to K$, $f(p(x)) = p(\alpha)$. Es más, $F[\alpha]$ es un cuerpo y f induce un isomorfismo de extensiones de F,*

$$\frac{F[x]}{(p(x))} \cong F[\alpha].$$

En particular,

$$[F[\alpha] : F] = \textit{grado } \alpha.$$

Demostración. El homomorfismo f está bien definido por el principio de sustitución, ya que es el único tal que $f_{|_F}\colon F \hookrightarrow K$ es la inclusión y $f(x) = \alpha$.

Ser α algebraico equivale a $\ker f \neq (0)$, pues los elementos de $\ker f$ son los polinomios en $F[x]$ que tienen a α como raíz. En particular, $\ker f \subsetneq F[x]$ ya que los polinomios constantes no nulos no tienen raíces.

Supongamos que α tiene polinomio irreducible $p(x)$. Entonces $p(x) \in \ker f$, así que $(p(x)) \subset \ker f$. Como $F[x]$ es un DIP, $(p(x))$ es maximal por ser $p(x)$ irreducible, así que $(p(x)) = \ker f$.

Recíprocamente, supongamos que $\ker f = (p(x))$ (este ideal es principal porque $F[x]$ es un DIP). Por el primer teorema de isomorfía, f induce un isomorfismo

$$\overline{f}\colon \frac{F[x]}{(p(x))} \xrightarrow{\cong} F[\alpha].$$

Como $F[\alpha] \subset K$ es un dominio, el ideal $(p(x)) \subset F[x]$ es primo. Como $F[x]$ es un DFU, esto equivale a decir que $p(x)$ es irreducible. Podemos además suponer que es mónico, dividiendo por su coeficiente líder si fuera necesario. En estas condiciones hemos visto arriba que el cociente es un cuerpo, más cocretamente una extensión de F del mismo grado que $p(x)$. Esto implica que el anillo $F[\alpha]$ es también un cuerpo, por ser isomorfo al cociente. Es más, según vimos en el tema de factorización, el isomorfismo $\overline{f}$ se comporta sobre F como la identidad, por tanto es un isomorfismo de extensiones, así que el grado de $F[\alpha]$ sobre F es también el de $p(x)$. □

El siguiente corolario se basa en el hecho de que $F[x]$ es un dominio euclídeo. Su importancia estriba en que da un método para calcular el polinomio irreducible de un elemento algebraico sin necesidad de comprobar la irreducibilidad por otros métodos.

Corolario 3.1.1.17. *Dada una extensión $F \subset K$, el polinomio irreducible de un elemento algebraico $\alpha \in K$ es el polinomio mónico no nulo de menor grado en $F[x]$ que tiene a α como raíz.*

Corolario 3.1.1.18. *Dada una extensión $F \subset K$ y un elemento algebraico $\alpha \in K$ de grado n, $\{1, \alpha, \ldots, \alpha^{n-1}\} \subset F[\alpha]$ es una base como F-espacio vectorial.*

Demostración. El isomorfismo de extensiones del teorema anterior es también un isomorfismo de F-espacios vectoriales. Sabemos que $\{1, \bar{x}, \ldots, \bar{x}^{n-1}\}$ es una base de $F[x]/(p(x))$, donde $p(x)$ es el polinomio irreducible de α, así que su imagen, $\{1, \alpha, \ldots, \alpha^{n-1}\}$, es una base de $F[\alpha]$. □

Proposición 3.1.1.19. *Si $F \subset K$ es una extensión, $\alpha \in K$ y $q(x) \in F[x]$ es un polinomio no nulo que tiene a α como raíz, entonces el polinomio irreducible de α divide a $q(x)$, en particular el grado de α sobre F es menor o igual que el grado de $q(x)$.*

Demostración. Consideramos el homomorfismo $f\colon F[x] \to K$ del teorema anterior. Si $p(x)$ es el polinomio irreducible de α, $\ker f = (p(x))$. Como α es una raíz de $q(x)$, $q(x) \in \ker f$, así que $q(x)$ es un multiplo no nulo de $p(x)$. □

Ejemplo 3.1.1.20. (Grado de algunos elementos) Sea $F \subset K$ una extensión y $\alpha \in K$ un elemento algebraico.

- No hay elementos de grado 0 porque los polinomios no nulos de grado 0 no tienen raíces.
- El grado de α es 1 si y solo si $\alpha \in F$. En efecto, esto equivale a decir que α es raíz de un polinomio mónico de grado 1 en $F[x]$ (todos ellos irreducibles) que no puede ser otro que $x - \alpha$.
- El grado de α es 2 si y solo si $\alpha \notin F$ pero es raíz de un polinomio de grado 2 en $F[x]$.

- Dado $\alpha \in K$ tal que $\alpha \notin F$ pero $\alpha^2 \in F$, el grado de α es 2 y su polinomio irreducible es $x^2 - \alpha^2 \in F[x]$.
- Si $F \subset \mathbb{R}$, el grado de $i \in \mathbb{C}$ sobre F es 2 pues $i \notin F$ pero es raíz de $x^2 + 1 \in F[x]$, que es su polinomio irreducible.
- Si $n \in \mathbb{Z}$ es libre de cuadrados, el grado de $\sqrt{n} \in \mathbb{C}$ sobre $\mathbb{Q}$ es 2 pues $\sqrt{n} \notin \mathbb{Q}$ pero es raíz de $x^2 - n \in \mathbb{Q}[x]$.
- Si $p \in \mathbb{Z}$ es primo, el grado de $\sqrt[n]{p} \in \mathbb{C}$ sobre $\mathbb{Q}$ es n puesto que es raíz del polinomio irreducible $x^n - p \in \mathbb{Q}[x]$. Este polinomio es irreducible por el criterio de Eisenstein para el primo p. Hay por tanto números complejos, incluso reales, de grado cualquiera sobre $\mathbb{Q}$.
- Si $\mathbb{C} \subset K$ es una extensión, los únicos elementos algebraicos son los de $\mathbb{C}$ ya que los únicos polinomios irreducibles en $\mathbb{C}[x]$ son los de grado 1, así que todo elemento algebraico tiene grado 1. Deducimos por tanto que la única extensión finita de $\mathbb{C}$ es la trivial.

Veamos que los homomorfismos de extensiones de F preservan raíces de polinomios con coeficientes en F.

Proposición 3.1.1.21. *Dadas dos extensiones $F \subset K$ y $F \subset L$ del mismo cuerpo F y un homomorfismo de extensiones $f\colon K \to L$, si $\alpha \in K$ es raíz de un polinomio $p(x) \in F[x]$ entonces $f(\alpha) \in L$ también es raíz de $p(x)$.*

Demostración. Como $f\colon K \to L$ es un homomorfismo de extensiones, f deja fijo a F. Si $p(x) = a_n x^n + \cdots + a_1 x + a_0$ con $a_i \in F$ y $\alpha \in K$ es una raíz entonces

$$a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0,$$

por tanto

$$\begin{aligned} 0 &= f(0) \\ &= f(a_n \alpha^n + \cdots + a_1 \alpha + a_0) \\ &= f(a_n) f(\alpha)^n + \cdots + f(a_1) f(\alpha) + f(a_0) \\ &= a_n f(\alpha)^n + \cdots + a_1 f(\alpha) + a_0, \end{aligned}$$

así que $f(\alpha) \in L$ también es raíz de $p(x)$. □

Ejemplo 3.1.1.22. (Extensiones no isomorfas del mismo grado) Las extensiones $\mathbb{Q}[i]$ y $\mathbb{Q}[\sqrt{2}]$ de $\mathbb{Q}$ tienen grado 2 pero no son isomorfas porque el polinomio $x^2+1 \in \mathbb{Q}[x]$ tiene raíces en $\mathbb{Q}[i]$ pero no en $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$.

Proposición 3.1.1.23. *Dada una extensión $F \subset K$, $\alpha \in K$ es trascendente si y solo si hay un isomorfismo $F[x] \cong F[\alpha]$ que deja fijo a F.*

Demostración. En virtud del teorema anterior, el elemento α es trascendente si y solo si el homomorfismo $f\colon F[x] \to K$, $f(p(x)) = p(\alpha)$, tiene núcleo trivial. Por el primer teorema de isomorfía, esto equivale a que f induzca un isomorfismo

$$F[x] \cong \frac{F[x]}{(0)} \cong \operatorname{im} f = F[\alpha]$$

definido por la misma fórmula $p(x) \mapsto p(\alpha)$. Este isomorfismo obviamente deja fijo a F. □

Corolario 3.1.1.24. *Dada una extensión $F \subset K$ y $\alpha \in K$ tal que $F[\alpha]$ tiene dimensión finita como F-espacio vectorial, α es algebraico.*

Demostración. No puede ser trascendente porque el anillo de polinomios $F[x]$ no tiene dimensión finita sobre F.

□

Corolario 3.1.1.25. *Si $F \subset K$ es una extensión finita, todo $\alpha \in K$ es algebraico.*

Demostración. Es consecuencia de que $F[\alpha] \subset K$ es un sub-F-espacio vectorial.

□

Proposición 3.1.1.26. *Dadas dos extensiones consecutivas $F \subset K \subset L$, si $F \subset L$ es finita entonces también lo son $F \subset K$ y $K \subset L$.*

Demostración. Como K es un sub-F-espacio vectorial de L, si $F \subset L$ es finita entonces $F \subset K$ también. Es más, como $F \subset K$, cualquier conjunto de generadores de L como F-espacio vectorial también lo genera como K-espacio vectorial, así que $K \subset L$ también es finita.

□

Proposición 3.1.1.27. *Dadas dos extensiones finitas consecutivas $F \subset K \subset L$, $F \subset L$ es finita de grado*

$$[L : F] = [L : K][K : F].$$

Demostración. Dada una base $\{x_1, \ldots, x_p\} \subset K$ como F-espacio vectorial y una base $\{y_1, \ldots, y_q\} \subset L$ como K-espacio vectorial, afirmamos que

$$\{x_i y_j\}_{\substack{1 \leq i \leq p \\ 1 \leq j \leq q}} \subset L$$

es una base como F-espacio vectorial. Hemos de ver que todo elemento de L se puede expresar de manera única como combinación lineal de este conjunto con coeficientes en F. La base de L como K-espacio vectorial nos garantiza que todo $\alpha \in L$ se puede escribir de manera única como

$$\alpha = \beta_1 y_1 + \cdots + \beta_q y_q,$$

con $\beta_j \in K$. La base de K como F-espacio vectorial nos asegura que cada uno de estos coeficientes se puede expresar de manera única como

$$\beta_j = \gamma_{1j} x_1 + \cdots + \gamma_{pj} x_p$$

con $\gamma_{ij} \in F$. Por tanto

$$\alpha = \sum_{i=1}^{p} \sum_{j=1}^{q} \gamma_{ij} x_i y_j$$

y esta expresión es única.

□

Observación 3.1.1.28. En las condiciones del enunciado anterior, decimos que K es una **extensión intermedia** de $F \subset L$. Decimos que es **estricta** si ninguna de las dos inclusiones es una igualdad.

Corolario 3.1.1.29. *Dada una extensión $F \subset K$ y elementos algebraicos $\alpha_1, \ldots, \alpha_n \in K$, la extensión $F \subset F[\alpha_1, \ldots, \alpha_n]$ es finita.*

Demostración. Por inducción en n. Para $n = 1$ está probado en el teorema anterior. Supongamos que $F \subset F[\alpha_1, \ldots, \alpha_{n-1}] = L$ es finita. Como α_n es algebraico sobre F, también lo es sobre L, así que $L \subset L[\alpha_n] = F[\alpha_1, \ldots, \alpha_n]$ es finita. El corolario se deduce ahora de la proposición anterior. □

Ejemplo 3.1.1.30. ($\mathbb{Q}[\sqrt[3]{2}, i]$) Consideremos la extensión $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}, i]$. Tenemos que

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{Q}[\sqrt[3]{2}, i].$$

Ya hemos visto que la extensión $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}]$ tiene grado 3. Además, como $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$, la extensión $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{Q}[\sqrt[3]{2}, i]$ tiene grado 2. Por tanto

$$\begin{array}{rcl} [\mathbb{Q}[\sqrt[3]{2}, i] : \mathbb{Q}] & = & [\mathbb{Q}[\sqrt[3]{2}, i] : \mathbb{Q}[\sqrt[3]{2}]][\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] \\ & = & 2 \cdot 3 = 6. \end{array}$$

Corolario 3.1.1.31. *Dada una extensión $F \subset K$, el subconjunto $L \subset K$ formado por los elementos de K que son algebraicos sobre F es un subcuerpo tal que $F \subset L$.*

Demostración. Los elementos de F son algebraicos de grado 1 sobre F, así que $F \subset L$. Veamos que $L \subset K$ es un subanillo. Tenemos que $0, 1 \in F \subset L$. Dados $\alpha, \beta \in L$, por el corolario anterior $F \subset F[\alpha, \beta]$ es una extensión finita, así que todos sus elementos son algebraicos. Como $\alpha + \beta, \alpha\beta, -\alpha \in F[\alpha, \beta]$, deducimos que estos tres elementos son en efecto algebraicos. Esto prueba que $L \subset K$ es un subanillo. Además, si $\alpha \neq 0$ entonces $\alpha^{-1} \in F[\alpha, \beta]$, que por lo mismo será también algebraico, por tanto L es un cuerpo. □

Corolario 3.1.1.32. *Dadas extensiones $F \subset K \subset L$:*

- $[K : F] = [L : F] \Rightarrow K = L$.
- $[L : F] = [L : K] \Rightarrow F = K$.

Demostración. Usando la fórmula para el grado de extensiones consecutivas vemos que en el primero caso $[L : K] = 1$ y en el segundo $[K : F] = 1$, así que basta usar que la única extensión de grado 1 es la trivial. □

Corolario 3.1.1.33. *Si $F \subset K$ es una extensión de grado $[K : F] = p$ primo entonces no posee extensiones intermedias estrictas.*

Demostración. Dada una posible extensión intermedia $F \subset L \subset K$, tenemos que $p = [K : F] = [K : L][L : F]$. Por ser p primo esto implica que bien $[K : F] = [K : L]$ o bien $[K : F] = [L : F]$, es decir $F = L$ o $K = L$.

□

Corolario 3.1.1.34. *Dada una extensión finita $F \subset K$, el grado de cualquier $\alpha \in K$ divide a $[K : F]$.*

Demostración. Basta observar que tenemos extensiones sucesivas $F \subset F[\alpha] \subset K$ y por tanto $[K : F] = [K : F[\alpha]][F[\alpha] : F]$. □

Corolario 3.1.1.35. *Dada una extensión finita $F \subset K$, existe una cantidad finita de elementos $\alpha_1, \ldots, \alpha_n \in K$ tales que $K = F[\alpha_1, \ldots, \alpha_n]$, que denominamos **generadores** de K sobre F.*

Demostración. Por inducción en el grado. Si $[K : F] = 1$ no hay nada que demostrar pues $K = F$. Supongamos que $[K : F] = n > 1$ y que el resultado es cierto para extensiones de grado $<n$. Entonces, como la inclusión $F \subsetneq K$ es estricta ha de existir $\alpha_1 \in K$ tal que $\alpha_1 \notin F$. Por tanto $F \subsetneq F[\alpha_1] \subset K$. Esto implica que $[F[\alpha_1] : F] > 1$ así que

$$\begin{aligned} n &= [K : F] \\ &= [K : F[\alpha_1]][F[\alpha_1] : F] \\ &> [K : F[\alpha_1]]. \end{aligned}$$

Entonces, por hipótesis de inducción, han de existir $\alpha_2, \ldots, \alpha_n \in K$ tales que

$$\begin{aligned} K &= F[\alpha_1][\alpha_2, \ldots, \alpha_n] \\ &= F[\alpha_1, \ldots, \alpha_n]. \end{aligned}$$

□

En la siguiente sección veremos que, para extensiones contenidas en $\mathbb{C}$ basta uno.

3.1.2. Elementos primitivos. Recuerda que $\alpha \in \mathbb{C}$ es una **raíz múltiple** de $f(x) \in \mathbb{C}[x]$ si $(x - \alpha)^2 | f$.

Proposición 3.1.2.1. *Un polinomio $f(x) \in \mathbb{C}[x]$ tiene una raíz múltiple $\alpha \in \mathbb{C}$ si y solo si α es raíz de f y de su derivada f'.*

Demostración. Sabemos que α es raíz de f si y solo si $(x - \alpha)|f$, es decir, si y solo si $f(x) = g(x)(x - a)$ para cierto $g(x) \in \mathbb{C}[x]$. Por tanto, α es una raíz múltiple de $f(x)$ si y solo si $(x - \alpha)|g$, es decir, si y solo si α es también una raíz de g. La derivada de f es

$$f'(x) = g'(x)(x - \alpha) + g(x),$$

luego $f'(\alpha) = g(\alpha)$, así que α es una raíz de f' si y solo si es raíz de g. □

Proposición 3.1.2.2. *Un polinomio $f(x) \in \mathbb{C}[x]$ tiene alguna raíz múltiple si y solo si f y f' no son coprimos.*

Demostración. $\Rightarrow$ Si α es una raíz múltiple de f, hemos visto antes que también es raíz de f', por tanto $x - \alpha$ divide tanto a f como a f'.

$\Leftarrow$ Si f y f' no son coprimos, entonces $\mathrm{mcd}(f, f') = g(x)$ es un polinomio no constante. Como $\mathbb{C}$ es algebraicamente cerrado, $g(x)$ tiene alguna raíz $\alpha \in \mathbb{C}$. Es más, como $g|f$ y $g|f'$, α también es raíz de f y de f', luego es una raíz múltiple de f. □

Proposición 3.1.2.3. *Dada una extensión $F \subset \mathbb{C}$, si $f(x) \in F[x]$ es irreducible entonces f y f' son coprimos, en particular f no tiene raíces múltiples en $\mathbb{C}$.*

Demostración. Como f es irreducible, no es constante, así que $f' \neq 0$. Sea $g = \mathrm{mcd}(f, f')$. Si g no es constante, entonces g y f son asociados, ya que $g|f$ y f es irreducible. Podemos pues suponer que $g = f$. Entonces $f|f'$, pero esto es imposible porque $f' \neq 0$, así que el grado de f' es $<$ el grado de f. □

Definición 3.1.2.4. Dada una extensión finita $F \subset K$, decimos que $\alpha \in K$ es un **elemento primitivo** si $K = F[\alpha]$.

Como de costumbre, en el enunciado del siguiente resultado "casi todo" significa "todo menos una cantidad finita".

Lemma 3.1.2.5. *Dada una extensión finita $F \subset K$ tal que $K \subset \mathbb{C}$ y $K = F[\alpha, \beta]$, $\gamma = \beta + c\alpha$ es un elemento primitivo para casi todo $c \in F$.*

Demostración. Sean $f(x), g(x) \in F[x]$ los polinomios irreducibles de $\alpha, \beta \in K$, respectivamente. Supongamos que sus grados respectivos son $m, n \geq 1$. Sean $\alpha_1, \ldots, \alpha_m$ y $\beta_1, \ldots, \beta_n$ sus raíces en $\mathbb{C}$, con $\alpha = \alpha_1$ y $\beta = \beta_1$. Como f y g no tienen raíces múltiples por ser irreducibles, los α_i son todos distintos, y también los β_j. Dado $c \in F$, denotemos

$$\gamma_{ij} = \beta_j + c\alpha_i.$$

Veamos que, si $(i, j) \neq (k, l)$, la igualdad $\gamma_{ij} = \gamma_{kl}$ solo puede ser cierta para un único valor de $c \in F$. En efecto, esto es cierto pues equivale a

$$c(\alpha_i - \alpha_k) = \beta_l - \beta_j.$$

Si $i \neq k$ entonces $\alpha_i \neq \alpha_k$ y podemos despejar c, que sería única. Si $i = k$ entonces $j \neq l$, luego $\beta_l \neq \beta_j$ y no hay ningún valor de c que satisfaga la ecuación. Por tanto, para casi todos los $c \in F$, los γ_{ij} son todos distintos. Fijemos tal $c \in F$, necesariamente no nula, y demostremos que $\gamma = \gamma_{11}$ es un elemento primitivo.

Consideramos la extensión intermedia $F \subset F[\gamma] \subset F[\alpha, \beta]$. Bastará demostrar que $\alpha \in F[\gamma]$, ya que entonces también $\beta = \gamma - c\alpha \in F[\gamma]$, y por tanto tendríamos la otra inclusión $F[\gamma] \supset F[\alpha, \beta]$.

Como $g(x) \in F[x]$, $h(x) = g(\gamma - cx) \in F[\gamma][x]$. Tenemos que $\alpha \in \mathbb{C}$ es raíz de h ya que $h(\alpha) = g(\gamma - c\alpha) = g(\beta) = 0$. También es raíz de $f \in F[x]$, que es su polinomio mínimo. Veamos que no poseen más raíces complejas en común. En efecto, si algún otro α_i, $i > 0$, fuera raíz de h, entonces $0 = h(\alpha_i) = g(\gamma - c\alpha_i)$. Como las raíces de g son los β_j, tendríamos que $\gamma - c\alpha_i = \beta_j$, así que $\gamma_{11} = \beta_j + c\alpha_i = \gamma_{ij}$, lo cual es imposible porque $i \neq 1$. De aquí deducimos que $\mathrm{mcd}(f, h) = x - \alpha$ en $\mathbb{C}[x]$. El divisor común máximo de dos polinomios está bien definido salvo producto por constantes no nulas. Es más, divisor común máximo de dos polinomios en $F[\gamma][x]$ lo es también en $\mathbb{C}[x]$, ya que toda división euclídea en el primero lo es también en el segundo, así que que el resultado de aplicar el arlgoritmo de Euclides en el primero es también válido en el segundo. Esto demuestra que $x - \alpha \in F[\gamma][x]$, así que en efecto $ α∈F[γ]$. □

Teorema 3.1.2.6. (del elemento primitivo) *Toda extensión finita contenida en $\mathbb{C}$ posee un elemento primitivo.*

Demostración. Sea $F \subset K$ una extensión finita. Vimos al final de la sección anterior que estaba generada por una cantidad finita de elementos $\alpha_1, \ldots, \alpha_n \in K$, $K = F[\alpha_1, \ldots, \alpha_n]$. Demostraremos este teorema por inducción en el número n de generadores. Para $n = 1$ no hay nada que demostrar. Probémoslo para n generadores suponiendo el resultado cierto para $n - 1$. Aplicando la hipótesis de inducción, $F[\alpha_1, \ldots, \alpha_{n-1}] = F[\beta]$, así que $K = F[\beta, \alpha_n]$, que por el lema anterior posee un elemento primitivo. □

Este teorema es cierto bajo hipótesis mucho más generales, pero la prueba se complica.

3.1.3. Construcciones con regla y compás.

Definición 3.1.3.1. Un punto, recta o circunferencia del plano $\mathbb{R}^2$ se considera **construido** en los siguientes casos:

- Los puntos $(0,0)$ y $(1,0)$.

FIGURA 6. Puntos constructibles

- Las rectas que pasan por dos puntos construidos.

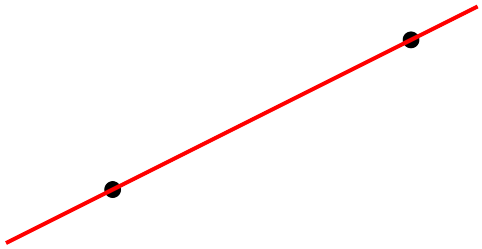

FIGURA 7. Recta constructible

- Las circunferencias de centro un punto construido que pasan por otro punto construido.

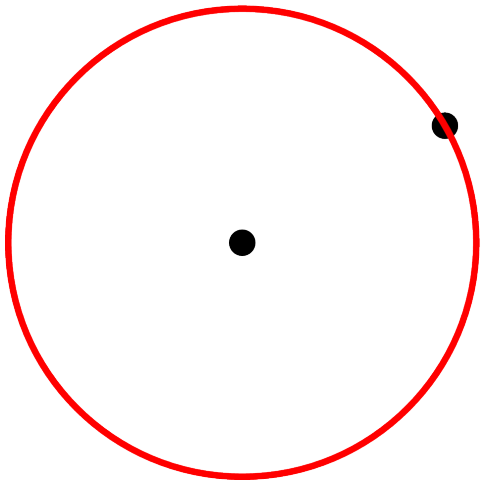

FIGURA 8. Circunferencia constructible

- El punto de intersección de dos rectas construidas.

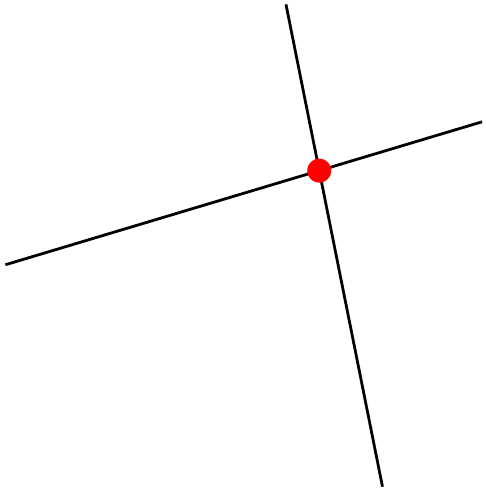

FIGURA 9. Intersección de rectas constructibles

- Los puntos de intersección de dos circunferencias construidas.

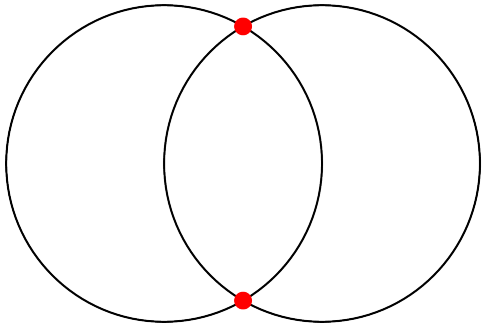

FIGURA 10. Intersección de circunferencias constructibles

- Los puntos de intersección de una recta y una circunferencia construidas.

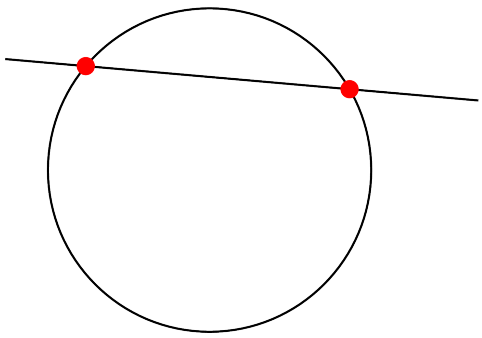

FIGURA 11. Intersección de recta y circunferencia constructible

Un número real $a \in \mathbb{R}$ es **constructible** si su valor absoluto $|a|$ es la distancia entre dos puntos constructibles.

Deducimos que además podemos construir:

- El punto medio entre dos puntos construidos.

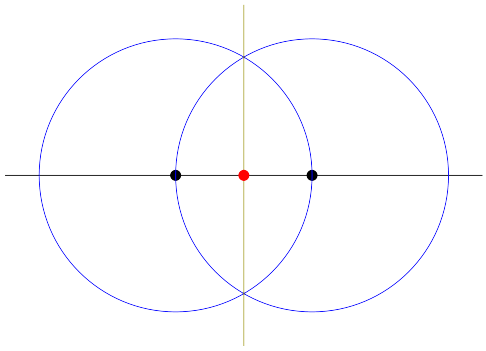

FIGURA 12. Punto medio

- La recta perpendicular a una recta construida que pasa por un punto consruido.

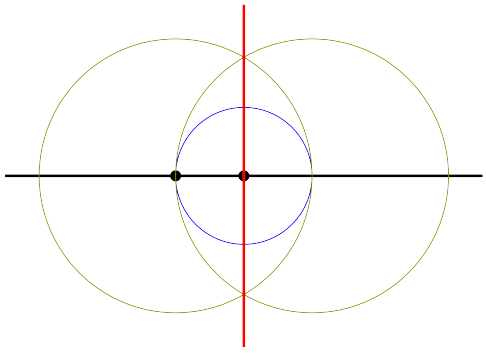

FIGURA 13. Perpendicular sobre un punto de la recta

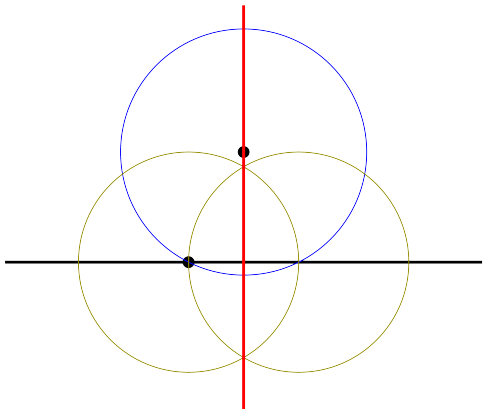

FIGURA 14. Perpendicular sobre un punto exterior

- La recta paralela a una recta construida que pasa por un punto consruido.

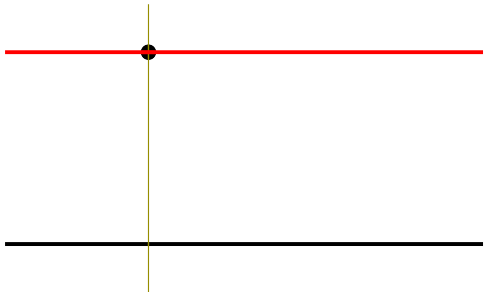

FIGURA 15. Paralela

- Los puntos que están a una distancia constructible de un punto construido dentro de una recta construida. Intuitivamente esta propiedad nos dice que podemos transportar distancias constructibles.

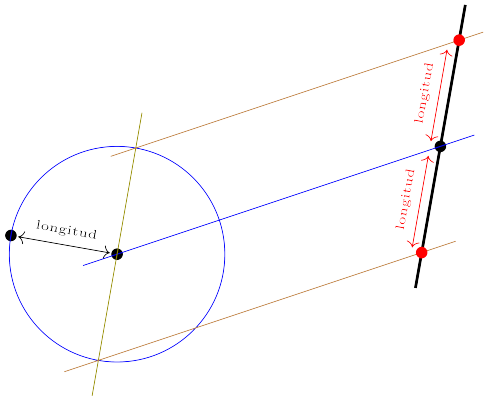

FIGURA 16. Transporte de longitud

Proposición 3.1.3.2. *Un punto $(a, b) \in \mathbb{R}^2$ es constructible si y solo si sus coordenadas $a, b \in \mathbb{R}$ son números constructibles.*

Demostración. $\Rightarrow$ Trazando paralelas y perpendiculares por puntos constructibles, podemos construir los ejes de coordenadas y las proyecciones de (a, b) sobre los mismos. La distancia de las proyecciones al origen son $|a|$ y $|b|$, así que las coordenadas son constructibles.

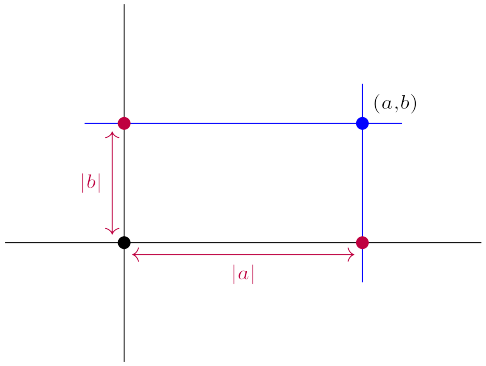

FIGURA 17. Coordenadas

$\Leftarrow$ Recíprocamente, asi a y b son constructibles podemos construir los puntos sobre los ejes de coordenadas que están a distancia $|a|$ y $|b|$ del origen, es decir, $(\pm a, 0)$ y $(0, \pm b)$, y obtener (a, b) como punto de intersección de las paralelas a los ejes que pasan por $(a, 0)$ y $(0, b)$. □

Proposición 3.1.3.3. *El subconjunto de $\mathbb{R}$ formado por los números constructibles es un cuerpo.*

Demostración. El 0 y el 1 son constructibles ya que el $(0, 0)$ y el $(1, 0)$ están construidos.

Dados $a \geq b \geq 0$ constructibles, podemos construir $a + b$ y $a - b$ tomando a partir del origen puntos del eje horizonal a distancias a y b,

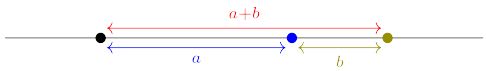

FIGURA 18. Suma

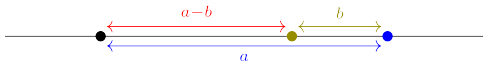

FIGURA 19. Resta

Por tanto también son constructibles $-a - b$ y $-a + b$. Esto demuestra que la suma de dos números constructibles cualesquiera y el opuesto de uno dado son constructibles.

Para construir el producto de dos números constructibles $a, b > 0$ usamos triángulos semejantes. Construimos primero el triángulo ractángulo con base en el eje horizontal, de longitud 1, vértice en el origen y altura a. El triángulo semejante de base b tiene altura ab.

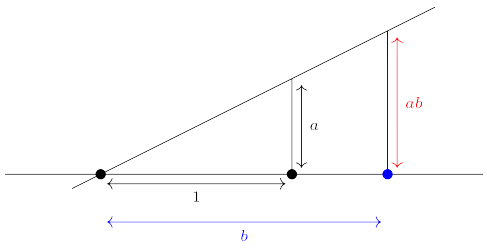

FIGURA 20. Producto

Esto demuestra que también son constructibles $(-a)b$, $a(-b)$ y $(-a)(-b)$, es decir, el producto de dos números constructibles cualesquiera (multiplicar por 0 da 0, que es constructible). Con esto hemos visto que los números constructibles forman un subanillo de $\mathbb{R}$.

La construcción del inverso de un número constructible $a > 0$ se lleva a cabo del mismo modo

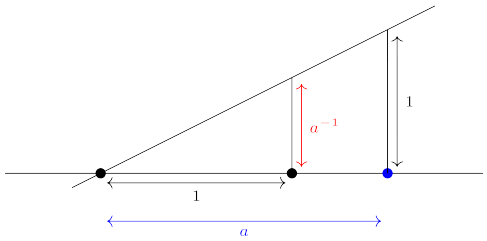

FIGURA 21. Inverso

Por tanto $(-a)^{-1} = -a^{-1}$ también es constructible. Esto demuestra que el anillo de los números constructibles es un cuerpo. □

Observación 3.1.3.4. El cuerpo de los números constructibles contiene a $\mathbb{Q}$ ya que está contenido en $\mathbb{R}$ y cualquier racional se puede obtener a partir del 1 sumando, tomando opuestos y dividiendo por números no nulos. Esto se aplica también a cualquier cuerpo contenido en $\mathbb{C}$ pero obviamente no es válido para los cuerpos finitos $\mathbb{Z}/(p)$.

Proposición 3.1.3.5. *Si $a \in \mathbb{R}$ es positivo $a > 0$ y constructible entonces $\sqrt{a}$ también es constructible.*

Demostración. Es consecuencia del conocido teorema de la media geométrica. En el eje horizontal tomamos el punto a la izquierda del origen a distancia a. Trazamos una circunferencia que pase por él y que tenga centro en el punto medio entre este punto y el $(1, 0)$. La distancia del origen al punto de corte con la circunferencia de la perpendicular al eje horizontal es $\sqrt{a}$.

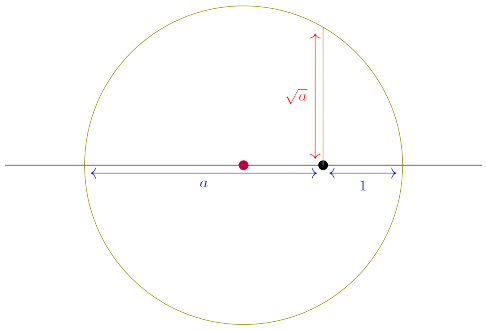

FIGURA 22. Raíz cuadrada

□

Hasta ahora hemos demostrado que podemos construir números constructibles a partir del 1 sumando, restando, dividiendo por números no nulos, y tomando raíces cuadradas de números positivos. Los siguientes resultados demuestras que no hay más números constructibles que los que se pueden obtener de este modo.

Proposición 3.1.3.6. *Dados cuatro puntos en $\mathbb{R}^2$ cuyas coordenadas están en un subcuerpo $F \subset \mathbb{R}$, los puntos de intersección de las rectas y circunferencias que se pueden dibujar apoyándose en dichos puntos tienen coordenadas en F o en $F[\sqrt{r}]$ para cierto $r \in F$ positivo $r > 0$ que no sea el cuadrado de ningún número de F.*

Demostración. Dados dos puntos $(a_0, b_0), (a_1, b_1) \in \mathbb{R}^2$, la recta que pasa por ambos tiene ecuación

$$(a_1 - a_0)(y - b_0) = (b_1 - b_0)(x - a_0),$$

y la circunferencia de centro el primero que pasa por el segundo está definida por

$$(x - a_0)^2 + (y - b_0)^2 = (a_1 - a_0)^2 + (b_1 - b_0)^2.$$

Si las coordenadas está en F entonces los coeficientes de ambas ecuaciones también.

La intersección de dos de estas rectas tiene coordenadas en F porque las soluciones de un sistema de ecuaciones lineales con coeficientes en un cuerpo siempre están en dicho cuerpo.

Para hallar la intersección de una recta y una circunferencia, despejamos una incógnita de la ecuación de la recta y la sustituimos en la ecuación de la circunferencia. Esto nos da una ecuación de grado 2 con coeficientes en F. Para que esta ecuación tenga solución su discriminante ha de ser $D \geq 0$. En ese caso la solución está en $F[\sqrt{D}]$. Por tanto las coordenadas del punto de intersección están en este cuerpo. Si D es el cuadrado de un número de F entonces $F[\sqrt{D}] = F$.

Para intersecar dos circunferencias, observamos que la diferencia de ambas ecuaciones es de grado 1, por tanto este caso se reduce al anterior.

□

Recuerda que antes hemos visto que $[F[\sqrt{r}] : F] = 2$ si $r \in F$ y $\sqrt{r} \notin F$.

Teorema 3.1.3.7. *Dados números reales constructibles $a_1, \dots, a_m \in \mathbb{R}$, hay una cadena de extensiones*

$$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = K$$

tales que

- $K \subset \mathbb{R}$ *es un subcuerpo,*
- $a_1, \dots, a_m \in K$*,*
- *Cada* $F_{i+1} = F_i[\sqrt{r_i}]$*,* $0 \leq i < n$*, donde* $r_i \in F_i$ *es un número positivo* $r_i > 0$ *que no es un cuadrado en* F_i*.*

En particular $[K : \mathbb{Q}] = 2^n$*.*

Demostración. La construtibilidad de los números a_i equivale a la de los puntos $(a_i, 0)$. Los puntos constructibles se construyen a partir de los básicos, $(0, 0)$ y $(1, 0)$, trazando e intersecando rectas y circunferencias mendiante los métodos permitidos. Los puntos básicos tienen coordenadas en $\mathbb{Q}$. Por la propisición anterior, los puntos que se construyen a partir de ellos tendrán coordenadas en extensiones sucesivas de $\mathbb{Q}$ obtenidas al añadir nuevas raíces cuadradas de números positivos, por tanto el teorema se sigue de la proposición anterior por inducción. La observación sobre el grado se siguie de la fórmula del grado para extensiones intermedias, que en este caso nos dice que

$$[K : \mathbb{Q}] = \prod_{i=0}^{n-1} [F_{i+1} : F_i] = 2^n$$

ya que por el tercer apartado $[F_{i+1} : F_i] = 2$. □

La cantidad de raíces cuadradas que hemos de añadir a $\mathbb{Q}$ para construir K (n según la notación del teorema) no tiene relación con la cantidad de números constructibles $a_1, \dots, a_m$ que queremos que K posea.

Corolario 3.1.3.8. *Los números constructibles son algebraicos sobre* $\mathbb{Q}$ *y el grado de un número constructible es siempre una potencia de* 2*.*

Demostración. Por el teorema anterior, si $a \in \mathbb{R}$ es constructible entonces $a \in K$ para cierta extensión finita $\mathbb{Q} \subset K$ de grado 2^n. En particular a es algebraico sobre $\mathbb{Q}$ y su grado divide a 2^n, así que ha de ser una potencia de 2. □

Ejemplo 3.1.3.9. (Números constructibles de grado 2^m cualquiera) Si $p \in \mathbb{Z}$ es un primo positivo, $\sqrt[n]{p}$ es constructible si y solo si n es una potencia de 2. Sabemos que este número tiene grado n sobre $\mathbb{Q}$, así que solo puede ser constructible si $n = 2^m$. Además en este caso podemos ver por inducción en m que de hecho es constructible. Para $m = 0$ es obvio porque es entero y si $\sqrt[2^{m-1}]{p}$ es constructible entonces

$$\sqrt[2^m]{p} = \sqrt{\sqrt[2^{m-1}]{p}}$$

también, por ser la raíz cuadrada de un número constructible.

Observación 3.1.3.10. Más adelante veremos que hay números cuyo grado es una potencia de 2 pero que no son constructibles, por ejemplo, las raíces reales del polinomio $x^4 - 6x + 3 \in \mathbb{Q}[x]$, que al ser irreducible tienen grado $4 = 2^2$.

Definición 3.1.3.11. Un ángulo $\theta \in [0, 2\pi)$ es **constructible** si el número $\cos\theta \in \mathbb{R}$ es constructible.

Por la construcción geométrica de senos y cosenos, está claro que la definición anterior es equivalente a decir que $\sin\theta$ es constructible, o que la recta que pasa por el origen y hace ángulo θ con el eje horizontal es constructible, o más generalmente que podemos construir la recta que pasa por un punto constructible y que hace ángulo θ con otra recta constructible que pasa por él.

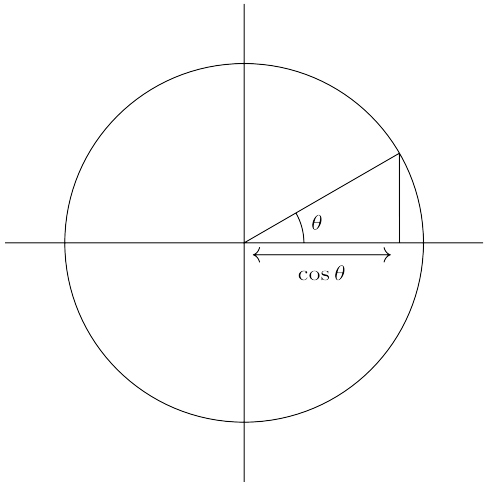

FIGURA 23. Ángulo constructible

Veamos que en general es imposible trisecar un ángulo cualquiera con regla y compás.

Proposición 3.1.3.12. *El ángulo de* 60 *es constructible pero su trisección no.*

Demostración. z Este ángulo se puede construir porque $\cos 60 = \frac{1}{2}$ es constructible. Cada ángulo de su trisección tendría 20 y el ángulo de 20 no es constructible. En efecto, la siguiente fórmula trigonométrica es cierta en general

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

Tomando $\theta = 20$ deducimos que $\alpha = \cos 20$ es una raíz del polinomio $8x^3 - 6x - 1$. Vamos a ver que este polinomio es irreducible sobre $\mathbb{Q}$, por tanto α tendrá grado 3 sobre $\mathbb{Q}$, así que no podrá ser constructible. El polinomio $8x^3 - 6x - 1$ es primitivo, por tanto es irreducible sobre $\mathbb{Q}$ si y solo si lo es sobre $\mathbb{Z}$. Sobre $\mathbb{Z}$ es irreducible por el criterio de reducción módulo 5, ya que $3x^3 - x - 1 \in \mathbb{Z}/(5)[x]$ tiene grado ≤ 3 pero no tiene raíces. □

Proposición 3.1.3.13. *Un polígono regular de p lados, $p \in \mathbb{Z}$ primo, puede construirse con regla y compás si y solo si $p = 2^n + 1$.*

Demostración. Esto equivale a la constructibilidad del ángulo de $\frac{2\pi}{p}$ radianes.

$\Leftarrow$ Es un resultado de Gauss que no probaremos.

$\Rightarrow$ El número complejo $\zeta = e^{\frac{2\pi i}{p}} = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ es una raíz p-ésima de la unidad, es decir, una raíz del polinomio $x^p - 1$. Este polinonimio factoriza como

$$(x-1)(x^{p-1} + \cdots + x + 1)$$

y como $\zeta \neq 1$, ζ es raíz del segundo, que se denomina p-ésimo **polinomio ciclotómico**

$$f(x) = x^{p-1} + \cdots + x + 1.$$

Veamos que este polinomio es irreducible sobre $\mathbb{Q}$. Para ello hacemos el cambio de variable $x = y + 1$, que se corresponde con el isomorfismo g que pasamos a definir.

Consideramos el único homomorfismo de anillos

$$g\colon \mathbb{Q}[x] \longrightarrow \mathbb{Q}[y]$$

tal que $g_{|\mathbb{Q}}$ es la inclusión $\mathbb{Q} \subset \mathbb{Q}[y]$ y $g(x) = y + 1$, que está bien definido por el principio de sustitución. El homomorfismo g está definido sobre un polinomio cualquiera $h(x) \in \mathbb{Q}[x]$ como $g(h(x)) = h(y + 1)$. Análogamente, consideramos el único homomorfismo

$$g'\colon \mathbb{Q}[y] \longrightarrow \mathbb{Q}[x]$$

tal que $g'_{|\mathbb{Q}}$ es la inclusión $\mathbb{Q} \subset \mathbb{Q}[x]$ y $g'(y) = x-1$. Sobre un polinomio cualquiera $h'(y) \in \mathbb{Q}[y]$, el homomorfismo g' está definido como $g'(h'(y)) = h'(x - 1)$. Es fácil comprobar que $g' \circ g = 1_{\mathbb{Q}[x]}$ y $g \circ g' = 1_{\mathbb{Q}[y]}$, por tanto g es un isomorfismo con inverso $g^{-1} = g'$. En particular, $f(x)$ es irreducible en $\mathbb{Q}[x]$ si y solo si $g(f(x)) = f(y + 1)$ es irreducible en $\mathbb{Q}[y]$. Vamos a probar esto último.

Como $x^p - 1 = (x - 1)f(x)$ entonces

$$\begin{aligned} yf(y+1) &= (y+1)^p - 1 \\ &= \textstyle\sum_{n=1}^{p} \binom{p}{n} y^n. \end{aligned}$$

Aplicando la propiedad cancelativa en el dominio $\mathbb{Q}[y]$ obtenemos que

$$p(y+1) = \textstyle\sum_{n=1}^{p} \binom{p}{n} y^{n-1}.$$

Este polinomio es irreducible por el criterio de Eisenstein para el primo p ya que el coeficiente líder es 1, el término independiente es p, y p divide a $\binom{p}{n}$ para todo $0<n<p$.

Por ser el polinomio ciclotómico $f(x)$ irreducible y tener a ζ como raíz, deducimos que ζ tiene grado $p - 1$ sobre $\mathbb{Q}$. Si $\frac{2\pi}{p}$ fuera constructible, tendríamos un cuerpo $K \subset \mathbb{R}$ tal que $\cos\frac{2\pi}{p}, \sin\frac{2\pi}{p} \in K$ y $[K : \mathbb{Q}] = 2^n$. Como K está contenido en los reales, $[K[i] : K] = 2$, luego $[K[i] : \mathbb{Q}] = [K[i] : K][K : \mathbb{Q}] = 2^{n+1}$. Además, $\zeta \in K[i]$ luego el grado de z, que es $p - 1$, ha de ser una potencia de 2. □

Ejemplo 3.1.3.14. (Primos de Fermat) Los enteros primos $p \in \mathbb{Z}$ tales que el polígono regular de p lados se puede construir con regla y compás, es decir los que son de la forma $p = 2^n + 1$, se denominan **primos de Fermat**. Solo se conocen los siguientes: 3, 5, 17, 257 y 65537. No se sabe siquiera si hay una cantidad finita o infinita de primos de Fermat. Este problema fue planteado por Eisenstein en 1844 y permanece abierto.

La siguiente imagen, obtenida de Wikipedia, muestra la construcción paso a paso de un polígono regular de 17 lados con regla y compás. En el artículo de Wikipedia enlazado se puede encontrar otra construccón de este polígono regular, así como una construcción completa del de 257 lados y el comienzo de la construcción del de 65537 lados.

FIGURA 24. Heptadecágono

3.2. Teoría de Galois

En esta sección supondremos sin necesida de mencionarlo explícitamente que todos los cuerpos que consideremos son subcuerpos de $\mathbb{C}$.

3.2.1. El grupo de Galois.

Definición 3.2.1.1. Dada una extensión $F \subset K$, su **grupo de Galois** $G(K/F)$ es el conjunto de los automorfismos de $F \subset K$.

Observación 3.2.1.2. La operación de grupo del grupo de Galois es la composición de automorfismos. El elemento unidad es la identidad. El grupo de Galois de la extensión trivial es el grupo trivial $G(F/F) = \{\mathrm{id}_F\}$. Recuerda que si la extensión $F \subset K$ es finita cualquier homomorfismo de extensiones $f\colon K \to K$ es un elemento de $G(K/F)$, y si además $F = \mathbb{Q}$ entonces cualquier homomorfismo de anillos $f\colon K \to K$ es un elemento de $G(K/F)$. Recuerda también que todo elemento de $G(K/F)$ es además un isomorfismo de F-espacios vectoriales, pero no todo isomorfismo de F-espacios vectoriales $f\colon K \to K$ está en $G(K/F)$ ya que podría no preservar el producto en K, o incluso el 1. Asimismo, recuerda que todo elemento de $G(K/F)$ preserva raíces de polinomios con coeficientes en F.

Ejemplo 3.2.1.3. ($G(\mathbb{C}/\mathbb{R})$) Un homomorfismo de $\mathbb{R}$-espacios vectoriales $f\colon \mathbb{C} \to \mathbb{C}$ está determinado por la imagen de los elementos de una base, por ejemplo $\{1, i\} \subset \mathbb{C}$. Para que $f \in G(\mathbb{C}/\mathbb{R})$ ha de ser un homomorfismo de anillos, así que debe satisfacer $f(1) = 1$. También ha de preservar raíces en $\mathbb{C}$ de polinomios en $\mathbb{R}[x]$. Las raíces complejas de $x^2 + 1$ son $\pm i$, así que f ha de cumplir $f(i) = \pm i$. Por tanto los dos posibles elementos de $G(\mathbb{C}/\mathbb{R})$ son los homomorfismos de $\mathbb{R}$-espacios vectoriales definidos por

$$\begin{aligned} f(1) &= 1, \\ f(i) &= i, \end{aligned}$$

y por

$$\begin{aligned} f(1) &= 1, \\ f(i) &= -i. \end{aligned}$$

Algunos de estos dos homomorfismos de $\mathbb{R}$-espacios vectoriales podría no estar en $G(\mathbb{C}/\mathbb{R})$ pues podría no preservar el producto, pero ambos lo preservan porque claramente el primero es la identidad $\mathrm{id}_{\mathbb{C}}$ y el segundo es la conjugación, que denotaremos c. Así que $G(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, c\}$, que es un grupo cíclico de orden 2 generado por la conjugación c, que satisface $c \circ c = \mathrm{id}_{\mathbb{C}}$.

Proposición 3.2.1.4. *Si $F \subset K$ es una extensión de grado $[K : F] = 2$ entonces $K = F[\sqrt{\delta}]$ para cierto $\delta \in F$ y $G(K/F) = \{\mathrm{id}_K, c\}$ es un grupo cíclico de orden 2 cuyo generador c denominamos **conjugación** y está caracterizado por satisfacer $c(\sqrt{\delta}) = -\sqrt{\delta}$.*

Demostración. Como la extensión no es trivial, ha de existir algún $\alpha \in K$ tal que $\alpha \notin F$. El grado de este elemento ha de dividir a 2. Como no puede ser 1 porque

$\alpha \notin F$, ha de ser 2. La extensión $F \subset F[\alpha]$ también tiene grado 2 y $F[\alpha] \subset K$ por tanto $K = F[\alpha]$. Si $x^2 + ax + b \in F[x]$ es el polinomio irreducible de α, entonces

$$\alpha = \frac{-a \pm \sqrt{\delta}}{2}$$

donde $\delta = a^2 - 4b \in F$ es el **discriminante**. Deducimos por tanto que $\sqrt{\delta} \in K$, $\sqrt{\delta} \notin F$, y $K = F[\sqrt{\delta}]$. Sabemos que $\{1, \sqrt{\delta}\} \subset K$ es una base como F-espacio vectorial. Como cualquier $f \in G(K/F)$ preserva el 1 y las raíces de $x^2 - \delta$, tenemos solo dos posibilidades:

$$\begin{aligned} f(1) &= 1, \\ f(\sqrt{\delta}) &= \sqrt{\delta}, \end{aligned}$$

y

$$\begin{aligned} f(1) &= 1, \\ f(\sqrt{\delta}) &= -\sqrt{\delta}. \end{aligned}$$

El primero es la identidad id_K, que es obviamente un isomorfismo de extensiones. El segundo es el que denominamos conjugación c. Dejamos como ejercicio probar que la conjugación, que a priori es solo un homomorfismo de F-espacios vectoriales, es de hecho un homomorfismo de extensiones. Solo queda por demostrar que preserva el producto. □

Ejemplo 3.2.1.5. ($G(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})$) Aquí $\sqrt[3]{2}$ denota la raíz cúbica de 2 real por lo que $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$. El resto de raíces cúbicas de 2 son puramente complejas. Cualquier $f \in G(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})$ ha de preservar las raíces de $x^3 - 2 \in \mathbb{Q}[x]$. La única raíz de este polinomio que está en $\mathbb{Q}[\sqrt[3]{2}]$ es $\sqrt[3]{2}$, ya que las otras dos están en $\mathbb{C} \setminus \mathbb{R}$, por tanto $f(\sqrt[3]{2}) = \sqrt[3]{2}$. Una base de $\mathbb{Q}[\sqrt[3]{2}]$ como $\mathbb{Q}$-espacio vectorial está formada por las primeras tres potencias de $\sqrt[3]{2}$, es decir, $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$. Como f ha de preservar la unidad y los productos, f tiene que mandar cada uno de los elementos de esta base a sí mismo, así que necesariamente $f = \mathrm{id}_{\mathbb{Q}[\sqrt[3]{2}]}$, por tanto en este caso el grupo de Galois es el tivial, $G(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}[\sqrt[3]{2}]}\}$ a pesar de que la extensión $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}]$ no es trivial, es de grado 3.

Definición 3.2.1.6. Dado un cuerpo F y un polinomio mónico no constante $p(x) \in F[x]$, el **cuerpo de descomposición** de $p(x)$ es $F[\alpha_1, \ldots, \alpha_n]$, donde $\alpha_1, \ldots, \alpha_n$ son las raíces complejas de $p(x)$.

Proposición 3.2.1.7. *Toda extensión $F \subset K$ de grado 2 es un cuerpo de descomposición.*

Demostración. Ya hemos visto que $K = F[\sqrt{\delta}]$ para cierto $\delta \in F$, entonces K es el cuerpo de descomposición de $x^2 - \delta$ ya que las raíces complejas de este polinomio son $\pm\sqrt{\delta}$ y $F[\sqrt{\delta}, -\sqrt{\delta}] = F[\sqrt{\delta}]$. □

El **grupo simétrico** de n letras, es decir el **grupo de permutaciones** de $\{1, \ldots, n\}$, se denotará S_n.

Proposición 3.2.1.8. *Dada una extensión $F \subset K$, si K es el cuerpo de descomposición de un polinomio $p(x) \in F[x]$ con n raíces distintas en K, entonces hay un único homomorfismo inyectivo*

$$\varphi\colon G(K/F) \longrightarrow S_n$$

tal que, si $\alpha_1, \ldots, \alpha_n \in K$ *son la raíces de* $p(x)$ *en* K *y* $f \in G(K/F)$*, la permutación* $\varphi(f) = \sigma$ *es la única que satisface la siguiente ecuación para todo* $i = 1, \ldots, n$*,*

$$f(\alpha_i) = \alpha_{\sigma(i)}.$$

Demostración. Como f preserva raíces de polinomios con coeficientes en F, f ha de mandar el conjunto $\{\alpha_1, \ldots, \alpha_n\}$ dentro de sí mismo. Además ha de hacerlo de manera biyectiva por ser f un automorfismo, por tanto existe una única permutación $\sigma \in S_n$ que satisface la ecuación del enunciado. Esto me permite definir la aplicación φ de manera única.

Veamos que φ es un homomorfismo de grupos. Por un lado $\varphi(\mathrm{id}_K)$ es la permutación identidad ya que $\mathrm{id}_K(\alpha_i) = \alpha_i$. Por otro lado, dados $f, g \in G(K/F)$, si denotamos $\varphi(f) = \sigma$ y $\varphi(g) = \tau$ entonces

$$\begin{aligned}(f \circ g)(\alpha_i) &= f(g(\alpha_i)) \\ &= f(\alpha_{\tau(i)}) \\ &= \alpha_{\sigma(\tau(i))} \\ &= \alpha_{(\sigma\circ\tau)(i)}.\end{aligned}$$

Por tanto

$$\begin{aligned}\varphi(f \circ g) &= \sigma \circ \tau \\ &= \varphi(f) \circ \varphi(g).\end{aligned}$$

Comprobemos por último que φ es inyectivo. Para ello debemos probar que si $f \in G(K/F)$ es tal que $\varphi(f)$ es le permutación identidad entonces $f = \mathrm{id}_K$. Por definición $\varphi(f)$ es la permutación identidad si y solo si $f(\alpha_i) = \alpha_i$ para todo $i = 1, \ldots, n$. Como $K = F[\alpha_1, \ldots, \alpha_n]$, todo elemento $\alpha \in K$ se puede escribir como polinomio en $\alpha_1, \ldots, \alpha_n$ con coeficientes en F, es decir

$$\alpha = \sum_{m_i \geq 0} b_{m_1,\ldots,m_n} \alpha_1^{m_1} \cdots \alpha_n^{m_n}$$

para ciertos $b_{m_1,\ldots,m_n} \in F$, casi todos nulos (y no necesariamente únicos, pero esto es irrelevante). Entonces

$$\begin{aligned}f(\alpha) &= f\left(\textstyle\sum_{m_i \geq 0} b_{m_1,\ldots,m_n} \alpha_1^{m_1} \cdots \alpha_n^{m_n}\right) \\ &= \textstyle\sum_{m_i \geq 0} f(b_{m_1,\ldots,m_n} \alpha_1^{m_1} \cdots \alpha_n^{m_n}) \\ &= \textstyle\sum_{m_i \geq 0} f(b_{m_1,\ldots,m_n}) f(\alpha_1)^{m_1} \cdots f(\alpha_n)^{m_n} \\ &= \textstyle\sum_{m_i \geq 0} b_{m_1,\ldots,m_n} \alpha_1^{m_1} \cdots \alpha_n^{m_n} \\ &= \alpha,\end{aligned}$$

así que $f = \mathrm{id}_K$. En las ecuaciones anteriores hemos usado que f es un homomorfismo de anillos que deja fijo a F y a las raíces $\alpha_1, \ldots, \alpha_n \in K$ de $p(x)$. □

Uno homomorfismo φ como el del enunciado se denomina **representación** del grupo de Galois como grupo de permutaciones.

Proposición 3.2.1.9. *Dadas dos extensiones consecutivas* $F \subset L \subset K$*, tenemos que* $G(K/L) \subset G(K/F)$*.*

Demostración. En efecto, si $f\colon K \to K$ es un isomorfismo de anillos que deja fijo a L entonces también deja fijo a F ya que $F \subset L$. □

Los subgrupos del grupo de Galois nos permiten construir extensiones intermedias.

Definición 3.2.1.10. Dada una extensión $F \subset K$ y un subgrupo $H \subset G(K/F)$ definimos el **cuerpo fijo** de H del siguiente modo:

$$K^H = \{\alpha \in K \mid f(\alpha) = \alpha \ \forall f \in H\}.$$

Proposición 3.2.1.11. *Dada una extensión $F \subset K$ y un subgrupo $H \subset G(K/F)$, el cuerpo fijo K^H es un subcuerpo de K que contiene a F,*

$$F \subset K^H \subset K.$$

Demostración. El conjunto K^H está contenido en K por definición. Es más, cualquier $\alpha \in F$ satisface $f(\alpha) = \alpha$ para todo $f \in G(K/F)$, en particular para todo $f \in H$, por tanto $F \subset K^H$.

Veamos que $K^H \subset K$ es un subanillo. Obviamente $0, 1 \in F \subset K^H$. Si $\alpha, \beta \in K^H$ entonces, dado $f \in H$, como $f\colon K \to K$ es un homomorfismo de anillos,

$$\begin{aligned} f(\alpha+\beta) &= f(\alpha)+f(\beta) \\ &= \alpha+\beta, \\ f(-\alpha) &= -f(\alpha) \\ &= -\alpha, \\ f(\alpha\beta) &= f(\alpha)f(\beta) \\ &= \alpha\beta. \end{aligned}$$

Por tanto $\alpha+\beta, -\alpha, \alpha\beta \in K^H$. Además K^H es un cuerpo porque si $\alpha \neq 0$ entonces

$$\begin{aligned} f(\alpha^{-1}) &= f(\alpha)^{-1} \\ &= \alpha^{-1}. \end{aligned}$$

□

Proposición 3.2.1.12. *Dada una extensión $F \subset K$ y un subgrupo $H \subset G(K/F)$ tenemos que $H \subset G(K/K^H)$.*

Demostración. Es obvio porque, por definición de K^H, todos los automorfismos de la extensión que están en H dejan fijo a K^H. □

3.2.2. Funciones simétricas.

Definición 3.2.2.1. Dado un anillo R, un polinomio $f = f(u_1, \ldots, u_n) \in R[u_1, \ldots, u_n]$ y un elemento $\sigma \in S_n$. El polinomio $\sigma(f) \in R[u_1, \ldots, u_n]$ es

$$\sigma(f) = f(u_{\sigma(1)}, \ldots, u_{\sigma(n)}).$$

La **órbita** de f es el conjunto de polinomios

$$\{\sigma(f) \mid \sigma \in S_n\}.$$

Decimos que f es **simétrico** si $f = \sigma(f)$ para todo $\sigma \in S_n$.

Ejemplo 3.2.2.2. (Una permutación aplicada a un polinomio) Si tomamos el polinomio $f = 2u_1^2u_3^2 - 3u_2 \in \mathbb{Z}[u_1, u_2, u_3]$ y le aplicamos la permutacición

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3) \in S_3$$

obtenemos el polinomio

$$\sigma(f) = 2u_2^2u_1^2 - 3u_3.$$

Consideranto las $3! = 6$ permutaciones de S_3, puedes comprobar que la órbita de f es el conjunto

$$\{2u_1^2u_3^2 - 3u_2, 2u_2^2u_3^2 - 3u_1, 2u_1^2u_2^2 - 3u_3\}.$$

Observación 3.2.2.3. La órbita de un polinomio en n variables tiene como máximo $|S_n| = n!$ elementos. Es más, el número de elementos de la órbita divide a $n!$. La órbita de un polinomio es un conjunto unitario si y solo si es simétrico. Los polinomios simétricos forman un subanillo de $R[u_1, \ldots, u_n]$. La aplicación

$$\sigma\colon R[u_1, \ldots, u_n] \to R[u_1, \ldots, u_n]$$

definida arriba es, por el principio de sustitución, el único homomorfismo de anillos tal que $\sigma_{|_R}$ es la inlcusión $R \subset R[u_1, \ldots, u_n]$ y $\sigma(u_i) = u_{\sigma(i)}$. Dadas $\sigma, \tau \in S_n$ y $f \in R[u_1, \ldots, u_n]$,

$$\sigma(\tau(f)) = (\sigma\tau)(f),$$

por tanto el producto de permutaciones se corresponde con la composición de los homomorfismos inducidos. En particular, estos últimos son automorfismos ya que el inverso de σ será el definido por la permutación inversa σ^{-1}. Aquí usamos que la permutación identidad induce la identidad.

Definición 3.2.2.4. Los **polinomios simétricos** o **funciones simétricas elementales** en n variables $s_i \in R[u_1, \ldots, u_n]$ son:

$$\begin{aligned}
s_1 &= \sum_{1 \le i \le n} u_i = u_1 + u_2 + \cdots + u_n, \\
s_2 &= \sum_{1 \le i < j \le n} u_iu_j = u_1u_2 + u_1u_3 + \cdots + u_{n-1}u_n, \\
s_3 &= \sum_{1 \le i < j < k \le n} u_iu_ju_k = u_1u_2u_3 + \cdots + u_{n-2}u_{n-1}u_n, \\
&\vdots \\
s_n &= u_1 \cdots u_n.
\end{aligned}$$

Es decir, para cada $1 \le j \le n$,

$$s_j = \sum_{1 \le i_1 < \cdots < i_j \le n} u_{i_1} \cdots u_{i_j}.$$

Observación 3.2.2.5. Las funciones simétricas elementales en n variables son, salvo signo, los coeficientes del polinomio

$$\begin{aligned} P(x) &= (x-u_1)\cdots(x-u_n) \\ &= x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n \\ &= \sum_{i=0}^{n}(-1)^i s_i x^{n-i}. \end{aligned}$$

En la última línea denotamos $s_0 = 1$.

En particular, dado un polinomio mónico $f \in F[x]$ degrado n

$$\begin{aligned} P(x) &= x^n - a_1x^{n-1} + a_2x^{n-2} - \cdots + (-1)^n a_n \\ &= \sum_{i=0}^{n}(-1)^i a_i x^{n-i} \\ &= (x-\alpha_1)\cdots(x-\alpha_n) \end{aligned}$$

con $a_0 = 1$, cuyas n raíces complejas denotamos α_i, sus coeficientes se obtienen al aplicarle las funciones simétricas elementales a estas raíces,

$$a_i = s_i(\alpha_1, \ldots, \alpha_n).$$

Teorema 3.2.2.6. (de las funciones simétricas) *Dado un polinomio simétrico $g \in R[u_1, \ldots, u_n]$, existe un único polinomio $G \in R[z_1, \ldots, z_n]$ tal que $g = G(s_1, \ldots, s_n)$.*

Demostración. Por doble inducción, primero en el número de variables y luego en el grado.

Para una sola variable, el resultado es obviamente cierto par cualquier grado ya que $s_1 = u_1$ y basta tomar $G = g(z_1)$. También es obvio para polinomios de grado 0. Supongamos que es cierto para polinomios de hasta $n-1$ variables.

Consideramos el polinomio $g_0 = g(u_1, \ldots, u_{n-1}, 0)$. Por hipótesis de inducción existe $G_0 \in R[z_1, \ldots, z_{n-1}]$ tal que $g_0 = G_0(s'_1, \ldots, s'_{n-1})$, donde las $s'_i \in R[u_1, \ldots, u_{n-1}]$ son las funciones simétricas elementales en $n-1$ variables. El polinomio

$$p(u_1, \ldots, u_n) = g(u_1, \ldots, u_n) - G_0(s_1, \ldots, s_{n-1})$$

es simétrico pues los polinomios simétricos forman un subanillo de $R[u_1, \ldots, u_n]$. Por construcción,

$$p(u_1, \ldots, u_{n-1}, 0) = g_0 - G_0(s'_1, \ldots, s'_{n-1}) = 0$$

así que $u_n | p$. Como p es simétrico, esto implica que $u_i | p$ para todo $1 \leq i \leq n$, así que $s_n = u_1 \cdots u_n | p$. Ha de existir por tanto un polinomio $h \in R[u_1, \ldots, u_n]$ tal que $p = s_n h$. Al ser p y s_n simétricos, h es también simétrico. Como h es de menor grado que g, por hipótesis de inducción existe $H \in R[z_1, \ldots, z_n]$ tal que $h = H(s_1, \ldots, s_n)$. Al ser

$$\begin{aligned} g &= p + G_0(s_1, \ldots, s_{n-1}) \\ &= s_n H(s_1, \ldots, s_n) + G_0(s_1, \ldots, s_{n-1}) \end{aligned}$$

podemos tomar $G = z_n H + G_0$. □

Definición 3.2.2.7. El **discriminante** en n variables es el polinomio

$$D = \prod_{1 \leq i < j \leq n} (u_i - u_j)^2 = (u_1 - u_2)^2 \cdots (u_{n-1} - u_n)^2.$$

Observación 3.2.2.8. El discriminante es simétrico y, dados $\alpha_1, \ldots, \alpha_n$, tenemos que $D(\alpha_1, \ldots, \alpha_n) = 0$ si y solo si $\alpha_i = \alpha_j$ para ciertos $i \neq j$. Denotaremos $\Delta \in R[z_1, \ldots, z_n]$ al único polinomio tal que $D = \Delta(s_1, \ldots, s_n)$.

Ejemplo 3.2.2.9. (Discriminantes en pocas variables) Para $n = 1$ el discriminante es $D = 1$. Si $n = 2$, entonces

$$\begin{aligned} D &= (u_1 - u_2)^2 \\ &= (u_1 + u_2)^2 - 4u_1u_2 \\ &= s_1 - 4s_2. \end{aligned}$$

Recuerda que el discriminante de un polinomio de grado 2

$$x^2 - a_1x + a_2 = (x - \alpha_1)(x - \alpha_2)$$

es

$$a_1^2 - 4a_2 = \Delta(a_1, a_2) = D(\alpha_1, \alpha_2).$$

Lemma 3.2.2.10. *Dado $p_1 \in R[u_1, \ldots, u_n]$, si $\{p_1, \ldots, p_l\}$ es su órbita y $h \in R[w_1, \ldots, w_l]$ es simétrico entonces $h(p_1, \ldots, p_l) \in R[u_1, \ldots, u_n]$ también es simétrico.*

Demostración. Tomemos $\tau \in S_n$. Como la órbita es

$$S = \{\sigma(p_1) \mid \sigma \in S_n\}$$

y $\tau(\sigma(p_i)) = (\tau\sigma)(p_1) \in S$, deducimos que $\tau(S) \subset S$. Es más, como $\tau\colon R[u_1, \ldots, u_n] \to R[u_1, \ldots, u_n]$ es un automorfismo, $\tau_{|S}$ es una permutación de S. Por tanto, ha de existir $\tau' \in S_l$ tal que

$$\tau(p_i) = p_{\tau'(i)}$$

para todo i. Entonces tenemos que

$$\begin{aligned} \tau(h(p_1, \ldots, p_l)) &= h(\tau(p_1), \ldots, \tau(p_l)) \\ &= h(p_{\tau'(1)}, \ldots, p_{\tau'(l)}) \\ &= \tau'(h)(p_1, \ldots, p_l) \\ &= h(p_1, \ldots, p_l) \end{aligned}$$

por ser h simétrica. □

Teorema 3.2.2.11. (de descomposición) *Si K es el cuerpo de descomposición de $f \in F[x]$ y $g \in F[x]$ es mónico e irreducible y posee una raíz en K entonces todas las raíces complejas de g están en K.*

Demostración. Sean $\alpha_1, \ldots, \alpha_n$ las raíces complejas de f y β_1 la raíz de g que está en K. Como $\beta_1 \in K = F[\alpha_1, \ldots, \alpha_n]$, existe $p_1 \in F[u_1, \ldots, u_n]$ tal que $\beta_1 = p_1(\alpha_1, \ldots, \alpha_n)$. Sea $\{p_1, \ldots, p_l\}$ la órbita de p_1 y $\beta_i = p_i(\alpha_1, \ldots, \alpha_n) \in K$, $1 \leq i \leq l$.

Nuestro objetivo ahora es probar que las raíces complejas de g están entre los $\beta_1, \ldots, \beta_l \in K$. Para ello consideramos el polinomio

$$h(x) = (x - \beta_1) \cdots (x - \beta_l).$$

Supongamos que hemos probado que h tiene coeficientes en F. Como g es el polinomio irreducible de β_1 sobre F y β_1 también es raíz de h, deduciremos que

$g|h$ en $F[x]$, así que las raíces de g están entre las de h, que es lo que nos habíamos propuesto demostrar.

Para ver que h tiene coeficientes en F, tomamos las funciones simétricas elementales $s'_1, \dots, s'_l$ en l nuevas variables $w_1, \dots, w_l$. Los coeficientes de h son los

$$s'_i(\beta_1, \dots, \beta_l) = s'_i(p_1(\alpha_1, \dots, \alpha_n), \dots, p_l(\alpha_1, \dots, \alpha_n)).$$

Los polinomios $s'_i(p_1, \dots, p_l) \in F[u_1, \dots, u_n]$ son simétricos en las n variables $u_1, \dots, u_n$ por el lema anterior. Por el teorema de las funciones simétricas, existen $G_1, \dots, G_l \in F[z_1, \dots, z_n]$ tales que $G_i(s_1, \dots, s_n) = s'_i(p_1, \dots, p_l)$. Aquí $s_i \in F[u_1, \dots, u_n]$ son las funciones simétricas en las n variables $u_1, \dots, u_n$. Así que los coeficientes de h son

$$G_i(s_1(\alpha_1, \dots, \alpha_n), \dots, s_n(\alpha_1, \dots, \alpha_n)).$$

Sabemos que $s_i(\alpha_1, \dots, \alpha_n) \in F$ pues son los coeficientes de f. Como los G_i también tiene coeficientes en F, deducimos de la fórmula anterior que los coeficientes de h están en F. □

Definición 3.2.2.12. Dada una extensión $F \subset K$ y un subgrupo $H \subset G(K/F)$, la **órbita** de $\alpha \in K$ por H es

$$\{f(\alpha) \mid f \in H\}.$$

Teorema 3.2.2.13. *Dada una extensión $F \subset K$ y un subgrupo $H \subset G(K/F)$, $\beta_1 \in K$ es algebraico sobre K^H si y solo si la órbita de β_1 por H es finita. En dicho caso, si la órbita es $\{\beta_1, \dots, \beta_l\}$, el polinomio irreducible de β_1 sobre K^H es*

$$g(x) = (x - \beta_1) \cdots (x - \beta_l).$$

En particular el grado de β_1 sobre K^H es el número de elementos de su órbita.

Demostración. $\Leftarrow$ Cada $f \in H$ induce una permutación de $\{\beta_1, \dots, \beta_l\}$. Los coeficientes de g son funciones simétricas elementales evaluadas en los β_i, por tanto no varían al aplicar $f \in H$. Esto demuestra que estos coeficientes están en K^H, por tanto β_1 es algebraico sobre K^H.

$\Rightarrow$ Sea $h \in K^H[x]$ un polinomio que tenga β_1 como raíz. Todo elemento de $f \in H \subset G(K/K^H)$ envía raíces de un polinomio con coeficientes en K^H en otras raíces, por tanto toda la órbita de β_1 por H está formada por raíces de h. Como todo polinomio con coeficientes en un cuerpo tiene una cantidad finita de raíces, deducimos que la órbita es finita.

Hemos visto que cuando la órbita es finita el polinomio g tiene coeficientes en K^H y que todos los elementos de la órbita son también raices de cualquier otro polinomio $h \in K^H[x]$ que tenga β_1 como raíz. Esto prueba que $g|h$ en $K[x]$ y por tanto también en $K^H[x]$, así que efectivamente g es el polinomio irreducible de β_1 sobre K^H. □

Definición 3.2.2.14. Una extensión $F \subset K$ es **algebraica** si todo elemento de K es algebraico sobre F.

Hemos visto que las extensiones finitas son algebraicas. El recíproco no es cierto en general, pero sí bajo ciertas hipótesis.

Lemma 3.2.2.15. *Si $F \subset K$ es una extensión algebraica y el grado de los elementos de K sobre F está uniformemente acotado entonces la extensión es finita.*

Demostración. Vamos a probar que si no fuera finita entonces existirían elementos de grado arbitrariamente grande. Para ello construimos una sucesión estrictamente creciente de extensiones intermedias

$$F = F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq K$$

tales que $F_{i-1} \subsetneq F_i$ es finita del siguiente modo. Supuesto construido hasta F_{n-1}, tomamos un elemento $\alpha_n \in K \setminus F_{n-1}$ y definimos $F_n = F_{n-1}[\alpha_n]$. Como α_n es algebraico sobre F, también lo es sobre F_{n-1}, así que $F_{n-1} \subsetneq F_n$ es finita, y en consecuencia $F \subsetneq F_n$ también, así que $F_n \subsetneq K$. Por la fórmula del grado para extensiones intermedias $[F_n : F] \geq 2^n$, así que cualquier elemento primitivo de $F \subsetneq F_n$ tiene grado $\geq 2^n$. □

Teorema 3.2.2.16. (del cuerpo fijo) *Sea $F \subset K$ una extensión y $H \subset G(K/F)$ un subgrupo. La extensión $K^H \subset K$ es finita si y solo si el grupo H es finito, y en dicho caso $[K : K^H] = |H|$.*

Demostración. $\Leftarrow$ Se sigue del teorema anterior que la extensión $K^H \subset K$ es algebraica. Es más, el grado de cualquier elemento es el número de elementos de una órbita, por tanto es $\leq |H|$. El lema anterior implica pues que $K^H \subset K$ es finita.

$\Rightarrow$ Sea $\gamma \in K$ un elemento primitivo, $K = K^H[\gamma]$. Cualquier $f \in H$ dejan fijo a K^H, así que $f, g \in H$ son iguales si y solo si $f(\gamma) = g(\gamma)$. Esto demuestra que la órbita de γ tiene tantos elementos como H. Por tanto H ha de ser finito en virtud del teorema anterior.

Es más, continuando con el argument del párrafo previo, el teorema anterior también implica que el grado de γ sobre K^H ha de ser $|H|$, y al ser γ primitivo su grado coincide con $[K, K^H]$. □

Corolario 3.2.2.17. *Si $F \subset K$ es una extensión finita entonces $G(K/F)$ es un grupo finito y $|G(K/F)|$ divide a $[K : F]$.*

Demostración. Como $F \subset K^{G(K/F)} \subset K$ es una extensión intermedia, $K^{G(K/F)} \subset K$ es una extensión finita, así que por el teorema anterior $G(K/F)$ es finito y $|G(K/F)| = [K : K^{G(K/F)}]$, y por la fórmula del grado para extensiones intermedias este último número divide a $[K : F]$. □

3.2.3. Extensiones de Galois.

Definición 3.2.3.1. Una extensión finita $F \subset K$ es de **Galois** si $|G(K/F)| = [K : F]$.

Lemma 3.2.3.2. *Dada una extensión finita $F \subset K$ y un subgrupo $H \subset G(K/F)$, la extensión $K^H \subset K$ es de Galois y $H = G(K/K^H)$.*

Demostración. Sabemos que, en general, $H \subset G(K/K^H)$ es un subgrupo, así que $|H| \leq |G(K/K^H)|$. También sabemos que $|G(K/K^H)|$ divide a $[K : K^H] = |H|$, así que tenemos también la otra desigualdad $|G(K/K^H)| \leq |H|$. Esto prueba que $H = G(K/K^H)$, por tanto esta extensión es de Galois. □

Lemma 3.2.3.3. *Sea $F \subset K = F[\gamma_1]$ una extensión finita, $g \in F[x]$ es el polinomio irreducible de γ_1 y $\gamma_1, \ldots, \gamma_r \in K$ las distintas raíces de g en este cuerpo. Para*

cada $1 \leq i \leq n$ *existe un único* $f_i \in G(K/F)$ *tal que* $f_i(\gamma_1) = \gamma_i$. *Es más,* $G(K/F) = \{f_1, \ldots, f_r\}$.

Demostración. Todos los γ_i poseen el mismo grado sobre F ya que tienen el mismo polinomio irreducible g, por tanto $K = F[\gamma_i]$ para todo i. Sabemos que, para cada i, hay un único isomorfismo

$$h_i \colon \frac{F[x]}{(g)} \cong K$$

que deja fijo a K tal que $h(\bar{x}) = \gamma_i$. Por tanto, $f_i = h_i h_1^{-1} \in G(K/F)$ es el único que satisface la propiedad del enunciado. Todo elemento $f \in G(K/F)$ está determinado por $f(\gamma_1)$ y además preserva raíces de $g \in F[x]$, así que $G(K/F)$ consta necesariamente de los f_i anteriores. □

Teorema 3.2.3.4. *Dada una extensión finita* $F \subset K$, *los siguientes enunciados son equivalentes:*

1. $F \subset K$ *es de Galois.*
2. $F = K^{G(K/F)}$.
3. K *es el cuerpo de descomposición de un polinomio de* $F[x]$.

Demostración. Veamos 1. $\Leftrightarrow$ 2. Por el teorema del cuerpo fijo, $|G(K/F)| = [K : K^{G(K/F)}]$. Como $F \subset K^{G(K/F)} \subset K$, $|G(K/F)| = [K : F]$ si y solo si $F = K^{G(K/F)}$.

Probemos ahora que 1. $\Leftrightarrow$ 3. Sea $\gamma_1 \in K$ un elemento primitivo de $F \subset K$, $g \in F[x]$ su polinomio irreducible y L el cuerpo de descomposición de g. Sean $\gamma_1, \ldots, \gamma_n \in \mathbb{C}$ las distintas raíces complejas de g, de las cuales $\gamma_1, \ldots, \gamma_r \in K$ y el resto no están en K. Denotemos $n = [G : K]$. El grado de g es n. Como $K = F[\gamma_1]$ y $L = F[\gamma_1, \ldots, \gamma_n]$, $F \subset K \subset L$. Usando el lema anterior vemos que $F \subset K$ es de Galois $\Leftrightarrow r = n \Leftrightarrow$ todas las raíces complejas de g están en $K \Leftrightarrow K \supset L \Leftrightarrow K = L$ $\Leftrightarrow K$ es un cuerpo de descomposición. En el último paso hemos usado que g tiene una raíz en K. □

Corolario 3.2.3.5. *Toda extensión finita* $F \subset K$ *es una extensión intermedia* $F \subset K \subset L$ *de una extensión de Galois* $F \subset L$.

Demostración. Basta tomar L como el cuerpo de descomposición de un elemento primitivo de $F \subset K$. □

Corolario 3.2.3.6. *Si* $F \subset K$ *es una extensión de Galois y* $F \subset L \subset K$ *es una extensión intermedia entonces* $L \subset K$ *también es de Galois.*

Demostración. Basta observar que si K es el cuerpo de descomposición de $g \in F[x]$ entonces también es el cuerpo de descomposición de del mismo polinomio visto como polinomio con coeficientes en L, $g \in L[x]$. □

Teorema 3.2.3.7. (fundamental de la teoría de Galois) *Dada una extensión de Galois* $F \subset K$, *las siguientes aplicaciones son biyectivas y mutuamente inversas:*

$$\begin{array}{rcl} \{\textit{ext. intermedias } F \subset L \subset K\} & \longleftrightarrow & \{\textit{subgrupos } H \subset G(K/F)\}, \\ L & \mapsto & G(K/L), \\ K^H & \leftarrow & H. \end{array}$$

Demostración. Dado un subgrupo $H \subset G(K/F)$, ya hemos probado en un lema anterior que $H = G(K/K^H)$, así que la composición que empieza y acaba en la derecha es la identidad. Dada ahora una extensión intermedia $F \subset L \subset K$, acabamos de probar que $L \subset K$ es de Galois, así que por el teorema anterior $K^{G(K/L)} = L$. □

Observación 3.2.3.8. Observa que la correspondencia dada en el Teorema Fundamental da la vuelta a las inclusiones. Es decir, dados dos subgrupos $H' \subset H \subset G(K/F)$ tenemos que $K^{H'} \supset K^H$ y dadas extensiones intermedias $F \subset L \subset L' \subset K$ tenemos que $G(K/L) \supset G(K/L')$. El subgrupo trivial se corresponde con K y el total con F.

Corolario 3.2.3.9. *Toda extensión finita $F \subset K$ posee una cantidad finita de extensiones intermedias.*

Demostración. Cuando la extensión es de Galois el resultado es cierto porque el grupo $G(K/F)$, que es finito, tiene una cantidad finita de subgrupos, que se corresponden con las extensiones intermedias. Si $F \subset K$ no fuera de Galois, basta tomar $F \subset K \subset L$ con $F \subset L$ de Galois y observar que toda extensión intermedia de $F \subset K$ lo es también de $F \subset L$. □

Teorema 3.2.3.10. *Dada una extensión de Galois $F \subset K$ y una extensión intermedia $F \subset L \subset K$, $F \subset L$ es de Galois si y solo si el subgrupo $G(K/L) \subset G(K/F)$ es normal. En dicho caso*

$$\frac{G(K/F)}{G(K/L)} \cong G(L/F).$$

Demostración. Comenzaremos probando la equivalencia de la primera parte del enunciado.

Sea $\gamma_1 \in L$ un elemento primitivo, $L = F[\gamma_1]$, con polinomio irreducible $g \in F[x]$. Sean $\gamma_1, \ldots, \gamma_r \in K$ sus raíces complejas, que están en K porque es un cuerpo de descomposición y $\gamma_1 \in K$.

$\Rightarrow$ Por ser $F \subset L$ de Galois, L es el cuerpo de descomposición de g, así que $L = F[\gamma_1, \ldots, \gamma_r]$. Todo $f \in G(K/L)$ preserva raíces de g, por tanto se restringe $f_{|_L} : L \to L$ y esta restricción está determinada por $f(\gamma_1)$ que será algún γ_i. En particular $f_{|_L}$ es la identidad si y solo si $f(\gamma_1) = \gamma_1$.

Sea $h \in G(K/L)$ un elemento cualquiera. Para ver que este grupo es normal tenemos que probar que $f^{-1}hf \in G(K/F)$ deja fijo a L y por tanto $f^{-1}hf \in G(K/L)$, es decir, que hay que probar que $(f^{-1}hf)(\gamma_1) = 1$. Esto es cierto porque h deja fijo a L, así que

$$\begin{aligned}(f^{-1}hf)(\gamma_1) &= f^{-1}(h(f(\gamma_1))) \\ &= f^{-1}(h(\gamma_i)) \\ &= f^{-1}(\gamma_i) \\ &= \gamma_1.\end{aligned}$$

$\Leftarrow$ Si $F \subset L$ no fuera de Galois no podría ser el cuerpo de descomposición de g, así que alguna raíz de g no estaría en L. Supongamos que γ_i es tal raíz. Como $L = K^{G(K/L)}$ y $\gamma_i \notin L$, existe $h \in G(K/L)$ tal qye $h(\gamma_i) \neq \gamma_i$. Es más, como $F = K^{G(K/F)}$, las raíces de g son la órbita de γ_1 por $G(K/F)$, así que existe $f \in G(K/F)$ tal que $f(\gamma_1) = \gamma_i$. El elemento $f^{-1}hf \in G(K/F)$ no puede dejar fijo

a γ_1 ya que de lo contrario $\gamma_i = f(\gamma_1) = hf(\gamma_1) = h(\gamma_i) \neq \gamma_i$. Esto implica que $f^{-1}hf$ no deja fijo a L, luego $f^{-1}hf \in G(K/L)$.

Una vez establecida la equivalencia de la primera parte del enunciado, demostraremos el isomorfismo de la segunda. Supongamos pues que $F \subset L$ es de Galois. Hemos visto que entonces todo $f \in G(K/F)$ se restringe a L, es decir $f_{|_L} \in G(L/F)$. Esta restricción induce un homomorfismo de grupos

$$\begin{array}{ccc} G(K/F) & \longrightarrow & G(L/F), \\ f & \mapsto & f_{|_L}. \end{array}$$

Obviamente $G(K/L)$ está contenido en el núcleo de este homomorfismo ya que los elementos de $G(K/L)$ se restringen a la identidad sobre L. Este homomorfismo es sobreyectivo porque $G(L/F)$ tiene r elementos, uno por cada raíz γ_i de g determinado por $\gamma_1 \mapsto \gamma_i$, y además hemos visto que en $G(K/F)$ siempre hay elementos que satisfacen $\gamma_1 \mapsto \gamma_i$. Por el primer teorema de isomorfía y el teorema de Lagrange, el número de elementos del núcleo núcleo es

$$\frac{|G(K/F)|}{|G(L/F)|} = \frac{[K:F]}{[L:F]} = [K:L] = |G(K/L)|.$$

Por tanto $G(K/L)$ es todo el núcleo y el isomorfismo del enunciado es el definido por el homomorfismo de restricción y el primer teorema de isomorfía,

$$\begin{array}{ccc} \frac{G(K/F)}{G(K/L)} & \stackrel{\cong}{\longrightarrow} & G(L/F), \\ [f] & \mapsto & f_{|_L}. \end{array}$$

□

3.2.4. Extensiones ciclotómicas. Dado $n \geq 1$, las **raíces n-ésimas de la unidad** son las n raíces complejas diferentes del polinomio

$$x^n - 1,$$

que son

$$e^{\frac{2\pi i t}{n}}, \qquad 0 \leq t < n.$$

El conjunto formado por estos n números complejos es un grupo cíclico de orden n para la multiplicación, generado por la **raíz n-ésima primitiva**,

$$\zeta = \zeta_n = e^{\frac{2\pi i}{n}}.$$

Si $n = p$ es primo, cualquier raíz distinta de 1 genera estre grupo.

Proposición 3.2.4.1. *Dado un entero primo $p \geq 1$, la extensión $\mathbb{Q} \subset \mathbb{Q}[\zeta]$ es de Galois de grado $p-1$ y su grupo de Galois es cíclico.*

Demostración. El cuerpo de descomposición de $x^p - 1$ es

$$\mathbb{Q}[1, \zeta, \ldots, \zeta^{p-1}] = \mathbb{Q}[\zeta].$$

En efecto, $\supset$ es obvio y $\subset$ es consecuencia de que como $\zeta \in \mathbb{Q}[\zeta]$ entonces todas las potencias $\zeta^t \in \mathbb{Q}[\zeta]$, $0 \leq t < n$, también. Esto demuestra que $\mathbb{Q}[\zeta]$ es de Galois.

Sabemos que

$$x^p - 1 = (x-1)q(x)$$

donde

$$q(x) = x^{p-1} + \cdots + x + 1$$

es el p-ésimo polinomio ciclotómico, que según vimos es irreducible. Como $\zeta \neq 1$, ζ ha de ser raíz de $q(x)$, así que el grado de la extensión es $p-1$.

Para ver que el grupo de Galois es cíclico, definimos un homomorfismo

$$\psi\colon G(\mathbb{Q}[\zeta]/\mathbb{Q}) \longrightarrow (\mathbb{Z}/(p))^\times$$

que llega al grupo $(\mathbb{Z}/(p))^\times$ de unidades del cuerpo $\mathbb{Z}/(p)$. Este último grupo sabemos que es cíclico de orden $p-1$. Todo $f \in G(\mathbb{Q}[\zeta]/\mathbb{Q})$ preserva raíces de $q(x)$, así que

$$f(\zeta) = \zeta^i$$

para cierto $0<i<p$ único y dependiente de f. Definimos

$$\psi(f) = \bar{i}.$$

Acabamos de probar que esta aplicación está bien definida. Veamos ahora que es un homomorfismo. Dado $g \in G(\mathbb{Q}[\zeta]/\mathbb{Q})$, hay un único $0<j<p$ tal que

$$g(\zeta) = \zeta^j$$

y que define $\psi(g) = \bar{j}$. Entonces

$$\begin{aligned}(f\circ g)(\zeta) &= f(g(\zeta))\\ &= f(\zeta^j)\\ &= f(\zeta)^j\\ &= (\zeta^i)^j\\ &= \zeta^{ij}.\end{aligned}$$

Por tanto

$$\begin{aligned}\psi(f\circ g) &= \overline{ij}\\ &= \bar{i}\bar{j}\\ &= \psi(f)\psi(g).\end{aligned}$$

Esto demuestra que ψ es un homomorfismo.

Veamos que ψ es inyectivo. Si $f \in G(\mathbb{Q}[\zeta]/\mathbb{Q})$ es tal que

$$\psi(f) = \bar{1}$$

es porque

$$f(\zeta) = \zeta.$$

Como f actúa como la identidad sobre los racionales y sobre el generador de la extensión $\mathbb{Q}[\zeta]$, f ha de ser la identidad. Esto prueba que el núcleo de ψ es trivial, así que es un homomorfismo inyectivo. □

3.2.5. Extensiones de Kummer. Dado un cuerpo F, nuestro objetivo es estudiar el cuerpo de descomposición K del polinomio

$$q(x) = x^p - a \in F[x]$$

donde p es primo y a no tiene raíces p-ésmas en F. Si α es una raíz compleja de $q(x)$, entonces el conjunto de todas sus raíces es

$$\alpha, \zeta_p\alpha, \dots, \zeta_p^{p-1}\alpha,$$

donde ζ_p es la raíz p-ésima primitiva de la unidad, ya que todas son raíces del polinomio $q(x)$ anterior y son todas distintas, pues ζ_p tiene orden p para el producto. En particular si $\zeta_p \in F$ entonces $K = F[\alpha]$.

Proposición 3.2.5.1. *Si $\zeta_p \in F$ y $q(x) = x^p - a \in F[x]$ no tiene raíces en F entonces el cuerpo de descomposición K de $q(x)$ tiene grado p sobre F.*

Demostración. Sea α una raíz compleja de $q(x)$. Hemos observado que $K = F[\alpha]$ y α es una raíz de $q(x)$, que es de grado p, por tanto $[K : F] \leq p$. Al ser $F \subset K$ de Galois, para probar la otra desigualdad bastará ver que $[K : F] = |G(K/F)| \geq p$.

Como $\alpha \notin F = K^{G(K/F)}$, ha de existir algún $f \in G(K/F)$ tal que $f(\alpha) \neq \alpha$. Como f preserva raíces de polinomios en $F[x]$, $f(\alpha) = \zeta_p^i\alpha$ para cierto $0<i<p$. Usaremos esto para ver que las potencias f^j de f son diferentes para todo $0 \leq j<p$, así que $G(K/F)$ tendrá en efecto al menos p elementos. Para ello basta comprobar que cada una de estas potencias f^j manda α a un elemento diferente. Vamos a probar por inducción que

$$f^j(\alpha) = (\zeta_p^i)^j\alpha.$$

Todos estos elementos son diferentes ya que al ser p primo todas las potencias de ζ_p distintas de 1, por ejemplo ζ_p^i, tienen orden multiplicativo p, así que todos los $(\zeta_p^i)^j$ son diferentes para $0 \leq j<p$. Para $j = 1$ la ecuación anterior es obviamente cierta. Supongamos que es cierta para $j - 1$. Como $\zeta_p \in F$ entonces $f(\zeta_p) = \zeta_p$ ya que. Por tanto,

$$\begin{aligned} f^j(\alpha) &= f(f^{j-1}(\alpha)) \\ &= f((\zeta_p^i)^{j-1}\alpha) \\ &= (f(\zeta_p)^i)^{j-1}f(\alpha) \\ &= (\zeta_p^i)^{j-1}\zeta_p^i\alpha \\ &= (\zeta_p^i)^j\alpha. \end{aligned}$$

□

Observación 3.2.5.2. A posteriori vemos que, en las condiciones de la proposición anterior, $x^p - a$ es un polinomio irreducible, pues cualquiera de sus raíces complejas tiene grado p.

Sorprendentemente el resultado a anterior tiene un recíproco.

Teorema 3.2.5.3. *Si p es un primo, F es un cuerpo tal que $\zeta_p \in F$ y $F \subset K$ es una extensión de Galois de grado $[K : F] = p$ entonces $K = F[\alpha]$ para cierto $\alpha \in K$ que es raíz de un polinomio de la forma $x^p - a \in F[x]$.*

Demostración. Al ser la extensión de Galois $|G(K/F)| = [K : F] = p$, por tanto $G(K/F)$ es cíclico de orden p, así que todo $f \in G(K/F)$ distinto de la identidad genera el grupo de Galois,

$$G(K/F) = \{f^0, f^1, \ldots, f^{p-1}\}.$$

Ahora vamos a concentrarnos en el hecho de que f es un homomorfismo de F-espacios vectoriales. Como $f^p = \mathrm{id}_K$ tenemos que cualquier autovalor λ de f satisface $\lambda^p = 1$, es decir, sus autovalores son raíces p-ésimas de la unidad. Además f es diagonalizable, pues niguna potencia de una caja de Jordan de tamaño 2×2 o superior es la matriz identidad. Como f es diagonalizable y distinto de la identidad, tendrá que tener algún autovalor $\lambda \neq 1$. Este autovalor ha de ser forzosamente de la forma $\lambda = \zeta_p^i$ para cierto $0<i<p$.

Sea $\alpha \in K$ un autovector asociado a ζ_p^i,

$$f(\alpha) = \zeta_p^i \alpha.$$

Tenemos entonces que

$$\begin{aligned} f(\alpha^p) &= f(\alpha)^p \\ &= (\zeta_p^i \alpha)^p \\ &= (\zeta_p^i)^p \alpha^p \\ &= \alpha^p. \end{aligned}$$

Se deduce por inducción que $f^i(\alpha^p) = \alpha^p$ para todo $i \geq 1$, por tanto $\alpha^p \in K^{G(K/F)} = F$. Esto demuestra que $\alpha \in K$ es raíz del polinomio $x^p - \alpha^p \in F[x]$. Además, como $f(\alpha) \neq \alpha$ entonces $\alpha \notin F$ así que $F \subsetneq F[\alpha] \subset K$ y como $[K : F] = p$ es primo concluimos que $K = F[\alpha]$. □

Igual que antes, en las condiciones del enunciado de este teorema el polinomio $x^p - a$ es necesariamente irreducible.

Las extensiones del tipo que hemos estudiado en esta sección se denominan **extensiones de Kummer**.

3.2.6. Solubilidad por radicales.

Definición 3.2.6.1. Decimos que $\alpha \in \mathbb{C}$ es **soluble** sobre un cuerpo F si existe una cadena de extensiones

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = K$$

tal que $\alpha \in K$ y $F_{i+1} = F_i[\sqrt[s_i]{r_i}]$ para ciertos $r_i \in F_i$ y $s_i \geq 2$, $0 \leq i < n$.

Los números solubles sobre F son los que se obtienen a partir de números de F realizando iteradamente sumas, restas, productos, divisiones por números no nulos y raíces n-ésimas. Nuestro objetivo es saber cuándo podemos hallar las raíces de un polinomio $p(x) \in F[x]$ de este modo a partir de sus coeficientes, es decir, queremos saber cuándo las raíces de $p(x)$ son solubles sobre F. Veremos cómo hacerlo usando el grupo de Galois del cuerpo de descomposición de $p(x)$.

Observación 3.2.6.2. Como $\sqrt[st]{r} = \sqrt[s]{\sqrt[t]{r}}$, no hay pérdida de generalidad sin en la definición anterior suponemos que los s_i son todos primos.

Añadiendo las raíces de manera sucesiva vemos que si $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ son solubles entonces existe una cadena de extensiones como la de la definición tal que $\alpha_1, \ldots, \alpha_m \in K$.

Definición 3.2.6.3. Un grupo G es **soluble** si existe una cadena de subgrupos

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$$

tal que $G_i \subset G_{i+1}$ es un subgrupo normal con cociente G_{i+1}/G_i abeliano para todo $0 \leq i < n$.

La solubilidad es una buena propiedad porque permite probar por inducción que muchas propiedades de los grupos abelianos son también ciertas para los grupo solubles.

Observación 3.2.6.4. Los grupos abelianos son solubles. Los grupos simétricos S_2, S_3 y S_4 también, así como todos sus subgrupos. Sin embargo, S_n no es soluble para ningún $n \geq 5$, ni tampoco su subgrupo alternado $A_n \subset S_n$. La solubilidad se preserva por isomorfismos.

Lemma 3.2.6.5. *Dado un grupo G y un subgrupo normal N, G es soluble si y solo si lo son N y G/N.*

Demostración. Denotamos $p\colon G \twoheadrightarrow G \subset N$ a la proyección natural.
$\Rightarrow$ Si

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$$

es una cadena en las condiciones de la definición entonces las cadenas siguientes demuestran que N y G/N son solubles,

$$\{e\} = N \cap G_0 \subset N \cap G_1 \subset \cdots \subset N \cap G_n = N,$$
$$\{e\} = p(G_0) \subset p(G_1) \subset \cdots \subset p(G_n) = G/N.$$

Aquí usamos que, gracias al primer teorema de isomorfía,

$$\frac{N \cap G_{i+1}}{N \cap G_i} \subset \frac{G_{i+1}}{G_i} \cong \frac{p(G_{i+1})}{p(G_i)}.$$

$\Leftarrow$ Si N y G/N son solubles gracias a las cadenas

$$\{e\} = N_0 \subset N_1 \subset N_2 \subset \cdots \subset N_m = N,$$
$$\{e\} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n = G/N,$$

entonces G es soluble gracias a la cadena

$$\{e\} = N_0 \subset \cdots \subset N_m = p^{-1}(K_0) \subset \cdots \subset p^{-1}(K_m) = G.$$

Aquí usamos que, gracias al primer teorema de isomorfía,

$$\frac{p^{-1}(K_{i+1})}{p^{-1}(K_i)} \cong \frac{K_{i+1}}{K_i}.$$

□

Corolario 3.2.6.6. *Dos grupos G y H son solubles si y solo si $G \times H$ es soluble.*

Demostración. Basta usar el primer teorema de isomorfía para observar que $G \cong G \times \{e\} \subset G \times H$ es un subgrupo normal y $(G \times H)/(G \times \{e\}) \cong H$. □

Proposición 3.2.6.7. *Un grupo finito G es soluble si y solo si existe una cadena de subgrupos*

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$$

tal que $G_i \subset G_{i+1}$ es un subgrupo normal con cociente G_{i+1}/G_i de orden primo, $0 \leq i < n$.

Demostración. Antes que nada, observamos que la demostración del lema anterior también sirve para probar que si G es un grupo y $N \subset G$ es un subgrupo normal, entonces G satisface la condición del enunciado de esta proposición si y solo si N y G/N la cumplen. En particular, dos grupos G y H la satisfacen si y solo si el producto $G \times H$ la cumple. Partiendo de esto, abordamos ahora la prueba de esta proposición.

$\Leftarrow$ Es obvio porque todo grupo de orden primo es cíclico y por tanto abeliano.

$\Rightarrow$ Si $G = \mathbb{Z}/(p^n)$ basta tomar $G_i = (\bar{p}^{n-i})$, $0 \leq i < n$, ya que todos los subgrupos de G son normales por ser abelianos y $\bar{p}^{n-i} \in \mathbb{Z}/(p^n)$ tiene orden p^i, así que $|G_i| = p^i$ y por tanto

$$\begin{aligned} \left|\frac{G_{i+1}}{G_i}\right| &= \frac{|G_{i+1}|}{|G_i|} \\ &= \frac{p^{i+1}}{p^i} \\ &= p. \end{aligned}$$

Si G es abeliano el resultado también es cierto, ya que al ser finito sería un producto finito de grupos de la forma $\mathbb{Z}/(p^n)$, en virtud del segundo teorema de estructura.

En general, si G satisface la condición de solubilidad gracias a la cadena

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G,$$

vamos a probar por inducción que cada G_i satisface la condición del enunciado. Obviamente G_0 la satisface por ser trivial. Si G_i la cumple, como $G_i \subset G_{i+1}$ es normal y G_{i+1}/G_i la satisface por ser abeliano, tenemos que G_{i+1} también la cumple. □

Lemma 3.2.6.8. *Dados dos polinomios $f_1, f_2 \in F[x]$, si L_1 y L_2 son los cuerpos de descomposición de f_1 y f_2, respectivamente, y K es el cuerpo de descomposición de $f_1 f_2$ entonces $G(K/F)$ es isomorfo a un subgrupo de $G(L_1/F) \times G(L_2/F)$.*

Demostración. Tenemos que $F \subset L_1, L_2 \subset K$, ya que las raíces de un producto de dos polinomios son la unión de las raíces de los factores. Consideramos el homomorfismo

$$G(K/F) \longrightarrow \frac{G(K/F)}{G(K/L_1)} \times \frac{G(K/F)}{G(K/L_2)} \cong G(L_1/F) \times G(L_2/F)$$

definido en cada coordenada como la proyecció natural. El núcelo es $G(K/L_1) \cap G(K/L_2)$, es decir, los automorfismos de K que dejan fijas a las raíces tanto de f_1 como de f_2. Un automorfismo así deja fijas a las raíces de $f_1 f_2$ y por tanto a su cuerpo de descomposición K, así que tiene que ser la identidad. Como el núcleo es trivial, el homomorfismo es inyectivo y, en virtur del primer teorema de isomorfía, el dominio es isomorfo a un subgrupo del codominio. □

Lemma 3.2.6.9. *Si $p_1, \dots, p_m$ son enteros primos dos a dos entonces el grupo de Galois de la extensión de Galois $F \subset F[\zeta_{p_1}, \dots, \zeta_{p_m}]$ es abeliano.*

Demostración. Para $m = 1$ se prueba como en el caso $F = \mathbb{Q}$. Por inducción, si es cierto para $m - 1$ primos, nuestro grupo de Galois es isomorfo a un subgrupo del producto de los de $F \subset F[\zeta_{p_1}, \dots, \zeta_{p_{m-1}}]$ y $F \subset F[\zeta_{p_m}]$ en virtud del lema anterior. El producto de grupos abelianos es abeliano y los subgrupos de los grupos abelianos también. □

Teorema 3.2.6.10. *Sea $p(x) \in F[x]$ un polinomio con cuerpo de descomposición L. Las raíces complejas de $p(x)$ son todas solubles sobre F si y solo si $G(L/F)$ es un grupo soluble.*

Demostración. $\Leftarrow$ Denotamos $G = G(L/F)$. Sea

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$$

una cadena de subgrupos como en la proposición anterior.

Supongamos primero que F tiene todas las raíces primitivas de la unidad asociadas a los primos que aparecen como el orden de los cocientes G_{i+1}/G_i. En este caso basta considerar la cadena de extensiones

$$L = L^{G_0} \supset L^{G_1} \supset \cdots \supset L^{G_n} \supset F[\zeta_{p_1}, \dots, \zeta_{p_n}]F.$$

En efecto, el teorema sobre extensiones de Kummer garantiza que cada $L^{G_i} \supset L^{G_{i+1}}$ se obtiene añadiendo una raíz.

Si F no tuviera todas las raíces primitivas de la unidad mencionadas, denotamos F' y L' a los cuerpos obtenidos al añadírselas a F y a L, respectivamente. Por construcción, la extensión $F \subset F'$ se puede interpolar como en la definición de número soluble. El grupo $G(L'/L)$ es abeliano por el lema anterior y

$$\frac{G(L'/F)}{G(L'/L)} \cong G(L/F),$$

que es soluble, así que $G(L'/F)$ es soluble y su subgrupo normal $G(L'/F')$ también. Como F' posee todas las raíces primitivas de la unidad necesarias, el párrafo anterior demuestra que $F' \subset L'$ también se puede interpolar como en la definición de número soluble. Por tanto $F \subset L'$ también, concatenando ambas interpolaciones.

$\Rightarrow$ El argumento es muy parecido anterior. Lo dejamos como ejercicio. □

Universidad de Sevilla, Facultad de Matemáticas, Departamento de Álgebra, Avda. Reina Mercedes s/n, 41012 Sevilla, Spain

Email address: fmuro@us.es

URL: http://personal.us.es/fmuro