UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

Departamento de Álgebra, Geometría y Topología

TRABAJO FIN DE GRADO

Criterios de irreducibilidad de polinomios
en dominios de factorización única

Doble Grado en Matemáticas y Física

Autor: Alfonso Palomares Berbel

Dirigido por los Profesores:

Juan Ramón Delgado Pérez
José Francisco Fernando Galván
José Manuel Gamboa Mutuberría

Contenido

Introducción

A lo largo de todo el texto, supondremos que los anillos A son conmutativos y unitarios. Su elemento unidad se denota 1_A o simplemente 1 si no hay riesgo de confusión. El problema de decidir la irreducibilidad de un polinomio es difícil, y en su alta complejidad se apoyan los primeros sistemas criptográficos de clave pública. Además, los polinomios irreducibles son fundamentales en diversas áreas de las matématicas. Entre ellas citemos la Teoría de Galois, pues los polinomios mónicos irreducibles están asociados a las extensiones finitas de cuerpos, y la Geometría algebraica clásica, en la que se corresponden con las hipersuperficies conexas. El intento *a fuerza bruta* de resolución del problema para polinomios en una variable consiste en estudiar, dado $f = a_0 + a_1\mathtt{t} + \cdots + a_d\mathtt{t}^d \in A[\mathtt{t}]$ con $a_d \neq 0$, la existencia de enteros positivos m y n tales que $m + n = d$ y elementos $b_0, \ldots, b_m, c_0, \ldots, c_n \in A$ con $b_m, c_n \neq 0$, satisfaciendo la igualdad

$$a_0 + a_1\mathtt{t} + \cdots + a_d\mathtt{t}^d = (b_0 + a_1\mathtt{t} + \cdots + b_m\mathtt{t}^m)(c_0 + c_1\mathtt{t} + \cdots + c_n\mathtt{t}^n).$$

Esta igualdad equivale a un sistema formado por $d+1$ ecuaciones cuadráticas y $m+n+2 = d+2$ incógnitas, y con frecuencia es complicado decidir si tal sistema de ecuaciones admite soluciones en el anillo A.

Para eludir este proceder los matemáticos han desarrollado diversas estrategias. En la mayor parte de los casos se trata de obtener condiciones suficientes que, a pesar de su aparente especificidad, permiten deducir la irreducibilidad de algunos polinomios.

Dedicamos la Sección segunda a introducir las nociones que emplearemos en el resto del trabajo, analizar algunos casos particulares muy sencillos e introducir un par de estrategias elementales pero útiles: el Criterio de la traslación y el Criterio de la homotecia. El resultado más relevante es el Corolario I.15 en el que se demuestra que si K denota el cuerpo de fracciones de un dominio de factorización única A y $f \in A[\mathtt{t}]$ es un polinomio primitivo de grado al menos 1, entonces f es irreducible en $A[\mathtt{t}]$ si y sólo si es irreducible en $K[\mathtt{t}]$.

En la Sección tercera se presentan Criterios modulares. En algunos casos, por ejemplo si $A := \mathbb{Z}$, se trata de sustituir el estudio de la irreducibilidad de un polinomio $f \in \mathbb{Z}[\mathtt{t}]$ por la de alguna de sus *reducciones modulares,* esto es, la imagen de f vía el homomorfismo

$$\mathbb{Z}[\mathtt{t}] \to \mathbb{Z}_n[\mathtt{t}],\ \sum_{i=0}^{d} a_i\mathtt{t}^i \mapsto \sum_{i=0}^{d} (a_i + n\mathbb{Z})\mathtt{t}^i,$$

para una adecuada elección de n. Este proceder trata de sustituir un problema de naturaleza infinitista (por ser $\mathbb{Z}$ infinito el conjunto de candidatos a dividir a f en $\mathbb{Z}[\mathtt{t}]$ es infinito), por otros de naturaleza finitista, pues el conjunto de polinomios en $\mathbb{Z}_n[\mathtt{t}]$ de grado fijado es finito.

Las dos secciones anteriores, cuyo contenido hemos tratado de resumir, tienen carácter muy general, y en su exposición nos hemos guiado por [A], [AG] y [FG].

En la sección cuarta se expone un Criterio original de irreduciblidad de polinomios, el Corolario III.5, que se deduce del Lema III.2, también original, y que tiene por consecuencia inmediata el Criterio de Eisenstein. Otra demostración del Criterio de Eisenstein se deduce del Lema III.9, que también es original. En esta misma sección se demuestran el Criterio de Eisenstein modificado y el Criterio de Netto.

El Criterio de Cohn y algunos refinamientos suyos se estudian en la Sección quinta. En su versión original, este criterio afirma que si $a_0 + a_1 \cdot 10 + \cdots + a_d \cdot 10^d$ es la escritura en base 10 de un número primo y $d \geq 1$, entonces el polinomio $a_0 + a_1\mathtt{t} + \cdots + a_d\mathtt{t}^d$ es irreducible en $\mathbb{Z}[\mathtt{t}]$. Posteriormente se generalizó este resultado sustituyendo la base 10 por una base cualquiera $b \geq 2$. Este es el contenido del Teorema IV.9, cuya prueba se divide en dos: el caso $b \geq 3$ es el contenido del Teorema IV.14, mientras que el caso $b = 2$ se prueba en el Teorema IV.16. Esta sección concluye con la prueba del Teorema IV.20 que afirma que si $a_0 + a_1 b + \cdots + a_d b^d$ es la escritura en cierta base $b \geq 2$ de una potencia de un número primo p y el polinomio

$$f(\mathtt{t}) := a_0 + a_1\mathtt{t} + \cdots + a_d\mathtt{t}^d$$

cumple que $f'(b)$ no es múltiplo de p, entonces f es irreducible en $\mathbb{Z}[\mathtt{t}]$.

En la sección sexta se pone de manifiesto la profunda conexión entre polinomios irreducibles y análisis complejo mediante la demostración del Criterio de Perron, que constituye el Teorema V.3, que afirma que si $f(\mathtt{t}) := a_0 + a_1\mathtt{t} + \cdots + a_{d-1}\mathtt{t}^{d-1} + \mathtt{t}^d$ es un polinomio mónico con coeficientes en $\mathbb{Z}$ con $a_0 \neq 0$ y se cumple que

$$|a_{d-1}| > 1 + |a_{d-2}| + \cdots + |a_0|\,,$$

entonces f es irreducible en $\mathbb{Z}[\mathtt{t}]$.

En la sección séptima se demuestra la irreducibilidad en $\mathbb{Z}[\mathtt{t}]$ de los polinomios ciclotómicos Φ_n. El caso en que n es primo se resuelve muy fácilmente en la sección cuarta combinando el Criterio de Eisenstein y el de la traslación, pero el caso general requiere más trabajo.

Para terminar estudiamos en la sección octava dos criterios de irreducibilidad de curvas planas, esto es, de polinomios en dos variables con coeficientes en un cuerpo. Enunciamos y demostramos el Criterio de Gibson en VII.3 y el Criterio de Lenstra en VII.7.

Hemos ilustrado todos los resultados del trabajo con numerosos ejemplos y hemos tratado de describir, con tanta precisión como nos ha sido posible, el alcance de cada uno de los criterios expuestos en el mismo.

CAPÍTULO I

Generalidades

Fijamos en esta sección un anillo A. Para cada $a \in A$ denotamos $aA := \{ax : x \in A\}$ el *ideal generado por* a.

Definiciones I.1 (1) Un elemento no nulo $a \in A$ es un *divisor de cero* en A si existe $b \in A \setminus \{0\}$ tal que $ab = 0$. El anillo A es un *dominio* cuando no tiene divisores de 0.

(2) Un elemento $a \in A$ es una *unidad* en A si existe $b \in A$ tal que $ab = 1$. Se denota por $\mathcal{U}(A)$ el conjunto de las unidades de A, que es un grupo multiplicativo abeliano.

(3) Supongamos que A es un dominio. Se dice que $a \in A \setminus \mathcal{U}(A)$ es *irreducible* en A si no existen $b, c \in A \setminus \mathcal{U}(A)$ tales que $a = bc$. En caso contrario se dice que a es *reducible* en A.

(4) Sean $a, b \in A$. Se dice que a *divide* a b en A, o que b *es múltiplo* de a en A, y se escribe $a|b$, si $b \in aA$. La notación es ambigua porque no hace referencia al anillo A, pero el contexto nos lo indicará en cada situación. Se dice que $a, b \in A$ son *asociados* en A si $a|b$ y $b|a$. Esto significa, exactamente, que $aA = bA$.

(5) Sean $r \geq 2$ y $a_1, \ldots, a_r \in A$. Se dice que $d \in A$ es un *máximo común divisor* de $a_1, \ldots, a_r$ en A si cada $a_i \in dA$ y $d \in bA$ para todo $b \in A$ tal que $b|a_i$ para cada $i = 1, \ldots, r$. Se escribe $d = \mathrm{mcd}_A(a_1, \ldots, a_r)$.

Observaciones I.2 (1) Los elementos irreducibles en el anillo $\mathbb{Z}$ de los números enteros son los enteros de la forma $\pm p$, donde p es un número primo. Sus unidades son 1 y -1.

(2) Sean b, c dos máximos comunes divisores en A de $a_1, \ldots a_r \in A$. Entonces $b|c$ y $c|b$, es decir b y c son asociados. Denotaremos $\mathrm{mcd}_A(a_1, \ldots, a_r)$ a cualquier representante de los máximos comunes divisores, recordando que los restantes son asociados suyos.

(3) Sean a, b asociados en el dominio A. Entonces existen $s, t \in A$ tales que $a = sb$ y $b = ta$, luego $a(st - 1) = 0$. Así, si $a = 0$ también $b = 0$ y si $a \neq 0$, entonces $st = 1$, es decir, $s, t \in \mathcal{U}(A)$. En consecuencia, los asociados de un elemento en un dominio A se obtienen multiplicándolo por las unidades de A.

(4) Por lo anterior, los asociados de cada número entero $z \in \mathbb{Z} \setminus \{0\}$ son z y $-z$. Por convenio, dado un conjunto finito de números enteros no nulos $a_1, \ldots, a_r$ diremos que su máximo común divisor es el único entero positivo que cumple la Definición I.1 (5).

Introducimos ahora algunas nociones necesarias para la exposición de criterios de irreducibilidad en anillos de polinomios. Dado un polinomio $f := \sum_{i=0}^{d} a_i \mathtt{t}^i \in A[\mathtt{t}]$, donde A es un anillo y $a_d \neq 0$ se dice que $d := \deg(f)$ es el *grado* de f y que $a_d := \ell(f)$ es su coeficiente director. Si $a_d \in \mathcal{U}(A)$ de dice que f es *mónico*.

Observación I.3 Supongamos que A es un dominio. Entonces, dados $f, g \in A[\mathtt{t}]$ se tiene $\deg(fg) = \deg(f)+\deg(g)$. Esto implica que $A[\mathtt{t}]$ es también un dominio y que el polinomio f es unidad en $A[\mathtt{t}]$ si y sólo si $\deg(f) = 0$, esto es, $f \in A$, y f es unidad en A.

Observación I.4 Sean A un anillo, $f \in A[\mathtt{t}]$ un polinomio mónico y $g, h \in A[\mathtt{t}]$ tales que $f = gh$. Entonces g y h son mónicos.

En efecto, como f es mónico, $\ell(f) \in \mathcal{U}(A)$. Además $\ell(f) = \ell(g)\ell(h)$. Por tanto

$$1 = \big(\ell(f)^{-1}\ell(g)\big)\,\ell(h),$$

luego $\ell(h)$ es unidad y h es mónico. También lo es g pues $\ell(g) = \ell(f)\ell(h)^{-1} \in \mathcal{U}(A)$.

Proposición I.5 Sean A un dominio y $f \in A[\mathtt{t}]$ un polinomio mónico de grado $d = 2$ o $d = 3$. Entonces f es irreducible en $A[\mathtt{t}]$ si y sólo si f no tiene raíces en A.

Demostración. Como f es mónico podemos suponer, por la observación anterior, que si es producto de dos factores, $f = gh$, éstos son mónicos, y por ello f es reducible si y sólo si $\deg(g) \geq 1$ y $\deg(h) \geq 1$. Como $2 \leq d = \deg(f) = \deg(g) + \deg(h) \leq 3$, alguno de los factores tiene grado 1, digamos $g(\mathtt{t}) := \mathtt{t} - a \in A[\mathtt{t}]$, luego $f(a) = 0$.

Para el recíproco observamos que si $a \in A$ es una raíz de f, entonces existe $h \in A[\mathtt{t}]$ tal que $f(\mathtt{t}) = (\mathtt{t} - a) \cdot h(\mathtt{t})$, por lo que f es reducible en $A[\mathtt{t}]$. □

Observaciones I.6 (Primeros ejemplos) (1) Si K es un cuerpo los polinomios de grado 1 son irreducibles en $K[\mathtt{t}]$. Obsérvese que esto deja de ser cierto en anillos más generales; el polinomio $f(\mathtt{t}) := 2\mathtt{t} + 2$ es reducible en $\mathbb{Z}[\mathtt{t}]$ al ser producto de dos polinomios $g(\mathtt{t}) := 2$ y $h(\mathtt{t}) := \mathtt{t} + 1$, ninguno de los cuáles es invertible en $\mathbb{Z}[\mathtt{t}]$.

(2) Los únicos polinomios irreducibles en $\mathbb{C}[\mathtt{t}]$ son los de grado 1. En efecto, si $f \in \mathbb{C}[\mathtt{t}]$ y $\deg(f) \geq 2$, el Teorema Fundamental del Álgebra asegura que existe $a \in \mathbb{C}$ tal que $f(a) = 0$, luego existe $g \in \mathbb{C}[\mathtt{t}]$ con $\deg(g) = \deg(f) - 1 \geq 1$ tal que $f(\mathtt{t}) = (\mathtt{t} - a)g(\mathtt{t})$, por lo que f es reducible en $\mathbb{C}[\mathtt{t}]$.

(3) Para determinar los polinomios irreducibles de $\mathbb{R}[\mathtt{t}]$ conviene introducir algunas notaciones. Para cada polinomio $f := \sum_{j=0}^{d} a_j \mathtt{t}^j \in \mathbb{C}[\mathtt{t}]$ denotamos $\overline{f} := \sum_{j=0}^{d} \overline{a}_j \mathtt{t}^j \in \mathbb{C}[\mathtt{t}]$. Obsérvese que $\overline{\overline{f}} = f$ y dados $f, h \in \mathbb{C}[\mathtt{t}]$ se cumple la igualdad $\overline{fh} = \overline{f} \cdot \overline{h}$. Además, $f \in \mathbb{R}[\mathtt{t}]$ si y sólo si $f = \overline{f}$, y si escribimos cada $a_j := u_j + \mathtt{i}v_j$ donde $u_j, v_j \in \mathbb{R}$ e $\mathtt{i} := \sqrt{-1}$, los polinomios

$$f_1 := \sum_{j=0}^{d} u_j \mathtt{t}^j \in \mathbb{R}[\mathtt{t}] \quad \text{y} \quad f_2 := \sum_{j=0}^{d} v_j \mathtt{t}^j \in \mathbb{R}[\mathtt{t}]$$

cumplen que $f = f_1 + \mathtt{i}f_2$. Se comprueba inmediatamente que si $g_1, g_2 \in \mathbb{R}[\mathtt{t}]$ cumplen la igualdad $f = g_1 + \mathtt{i}g_2$, entonces $f_1 = g_1$ y $f_2 = g_2$.

(3.i) Sean $f \in \mathbb{C}[\mathtt{t}]$ y $u \in \mathbb{C}$ una raíz de f. Entonces $\overline{u}$ es raíz de $\overline{f}$ y las multiplicidades $\mathrm{mult}_u(f)$ y $\mathrm{mult}_{\overline{u}}(\overline{f})$ de u y de $\overline{u}$ como raíces de f y $\overline{f}$ coinciden.

En efecto, si $\mathrm{mult}_u(f) = m$ existe, por la Regla de Ruffini, $g \in \mathbb{C}[\mathtt{t}]$ tal que $g(u) \neq 0$ y $f(\mathtt{t}) = (\mathtt{t} - u)^m g(\mathtt{t})$, y por tanto,

$$\overline{f}(\mathtt{t}) = \big(\overline{(\mathtt{t} - u)}\big)^m \cdot \overline{g}(\mathtt{t}) = (\mathtt{t} - \overline{u})^m \cdot \overline{g}(\mathtt{t}),$$

así que $\mathrm{mult}_u(f) \leq \mathrm{mult}_{\overline{u}}(\overline{f})$. Aplicando esto a la raíz $v := \overline{u}$ de $h := \overline{f}$ resulta

$$\mathrm{mult}_{\overline{u}}(\overline{f}) = \mathrm{mult}_v(h) \leq \mathrm{mult}_{\overline{v}}(\overline{h}) = \mathrm{mult}_u(\overline{f}),$$

y en consecuencia, $\mathrm{mult}_u(f) = \mathrm{mult}_{\overline{u}}(\overline{f})$.

(3.ii) Si $u \in \mathbb{C}$ es raíz de $f \in \mathbb{R}[\mathtt{t}]$ también $\overline{u}$ es raíz de f y $\mathrm{mult}_u(f) = \mathrm{mult}_{\overline{u}}(f)$.

(4) Cada polinomio $f \in \mathbb{R}[\mathtt{t}]$ de grado 2 sin raíces reales es irreducible en $\mathbb{R}[\mathtt{t}]$. En efecto, en caso contrario sería producto de dos polinomios $g(\mathtt{t}) := a\mathtt{t} - b$ y $h(\mathtt{t})$ en $\mathbb{R}[\mathtt{t}]$ de grado 1, por lo que $f\big(\frac{b}{a}\big) = 0$, esto es, $\frac{b}{a} \in \mathbb{R}$ sería raíz de f, contra lo supuesto.

Los polinomios de grado 1 y los de grado 2 sin raíces reales son los únicos polinomios irreducibles en $\mathbb{R}[\mathtt{t}]$. De hecho si $f \in \mathbb{R}[\mathtt{t}]$ tiene grado ≥ 2 y alguna raíz $\alpha \in \mathbb{R}$, es reducible en $\mathbb{R}[\mathtt{t}]$ por ser múltiplo de $\mathtt{t} - \alpha$. Esto demuestra, en particular, la reducibilidad de los polinomos de grado 2 con alguna raíz real y, por el Teorema de Bolzano, la de los polinomios de grado impar mayor o igual que 3. Por último, sea $f \in \mathbb{R}[\mathtt{t}]$ de grado par mayor o igual que 4 sin raíces reales. Por el Teorema Fundamental del Álgebra f tiene una raíz $u := a + b\mathtt{i} \in \mathbb{C} \setminus \mathbb{R}$ y denotamos $\overline{u} = a - b\mathtt{i}$ su conjugado, que por (3.ii) es raíz de f. Por tanto, $\mathtt{t} - u$ y $\mathtt{t} - \overline{u}$ dividen a f en $\mathbb{C}[\mathtt{t}]$, por la Regla de Ruffini.

Además $\mathrm{mcd}_{\mathbb{C}[\mathtt{t}]}(\mathtt{t} - u, \mathtt{t} - \overline{u}) = 1$, pues si $d \in \mathbb{C}[\mathtt{t}]$ divide en $\mathbb{C}[\mathtt{t}]$ a $\mathtt{t} - u$ y a $\mathtt{t} - \overline{u}$, entonces d divide a la resta $\mathtt{t} - \overline{u} - (\mathtt{t} - u) = u - \overline{u} = 2b\mathtt{i}$, que es unidad en $\mathbb{C}[\mathtt{t}]$. En consecuencia, el producto

$$h(\mathtt{t}) := (\mathtt{t} - u)(\mathtt{t} - \overline{u}) = \big(\mathtt{t}^2 - (u + \overline{u})\mathtt{t} + u\overline{u}\big) = \mathtt{t}^2 - 2a\mathtt{t} + (a^2 + b^2) \in \mathbb{R}[\mathtt{t}]$$

divide en $\mathbb{C}[\mathtt{t}]$ a f, luego $f(\mathtt{t}) = g(\mathtt{t})h(\mathtt{t})$ para cierto $g \in \mathbb{C}[\mathtt{t}]$. Sea $g(\mathtt{t}) = g_1(\mathtt{t}) + \mathtt{i}g_2(\mathtt{t})$ donde $g_1, g_2 \in \mathbb{R}[\mathtt{t}]$. Entonces $f + 0\mathtt{i} = f = gh = (g_1 + \mathtt{i}g_2)h = g_1h + \mathtt{i}g_2h$, así que $f = g_1h$ es reducible en $\mathbb{R}[\mathtt{t}]$.

Al sustituir el anillo de coeficientes $\mathbb{R}$ o $\mathbb{C}$ por anillos más generales decidir si un polinomio es o no reducible es una cuestión más delicada y a la exposición de algunas soluciones parciales al problema está dedicado este trabajo.

Dos resultados muy elementales pero que combinados con otros proporcionan la irreducibilidad de algunos polinomios son los siguientes.

Proposición I.7 (Criterio de la traslación) *Sean A un anillo, $a \in A$ y*

$$\tau_a : A[\mathtt{t}] \to A[\mathtt{t}],\ f(\mathtt{t}) \mapsto f(\mathtt{t} + a).$$

(1) *La aplicación τ_a es un isomorfismo de anillos cuyo inverso es τ_{-a}.*

(2) *Para cada $f \in A[\mathtt{t}]$, las siguientes afirmaciones son equivalentes:*

(2.1) *El polinomio f es irreducible en $A[\mathtt{t}]$.*

(2.2) *El polinomio $f(a + \mathtt{t})$ es irreducible en $A[\mathtt{t}]$ para cada $a \in A$.*

(2.3) *Existe $a \in A$ tal que el polinomio $f(a + \mathtt{t})$ es irreducible en $A[\mathtt{t}]$.*

Demostración. (1) La comprobación de que τ_a es homomorfismo es inmediata y también lo es que $\tau_a \circ \tau_{-a}$ es la identidad.

(2) Basta aplicar (1) y que los isomorfismos preservan la irreduciblidad. □

Proposición I.8 (Criterio de la homotecia) *Sean A un anillo, $a \in \mathcal{U}(A)$ y*

$$\sigma_a : A[\mathtt{t}] \to A[\mathtt{t}],\ f(\mathtt{t}) \mapsto f(a\mathtt{t}).$$

(1) *La aplicación σ_a es un isomorfismo de anillos cuyo inverso es $\sigma_{a^{-1}}$.*

(2) *Para cada $f \in A[\mathtt{t}]$, las siguientes afirmaciones son equivalentes:*

(2.1) *El polinomio f es irreducible en $A[\mathtt{t}]$.*

(2.2) *El polinomio $f(a\mathtt{t})$ es irreducible en $A[\mathtt{t}]$ para cada $a \in \mathcal{U}(A)$.*

(2.3) *Existe $a \in \mathcal{U}(A)$ tal que el polinomio $f(a\mathtt{t})$ es irreducible en $A[\mathtt{t}]$.*

Demostración. (1) La comprobación de que σ_a es homomorfismo es inmediata y también lo es que $\sigma_a \circ \sigma_{a^{-1}}$ es la identidad.

(2) Basta aplicar (1) y que los isomorfismos preservan la irreduciblidad. □

Los problemas relativos a la de irreducibilidad de polinomios son especialmente interesantes cuando el anillo de coeficientes es un *dominio de factorización única,* y serán los que trataremos en este trabajo. Recordemos antes algunas nociones y resultados acerca de estos anillos.

Definiciones I.9 Se dice que un dominio A es un *dominio de factorización única* (y se abrevia diciendo que A es un DFU) si para cada elemento no nulo $a \in A$ que no es unidad en A se cumplen las siguientes condiciones:

(i) Existe una cantidad finita de elementos irreducibles $p_1, \ldots, p_r \in A$, no necesariamente distintos, tales que $a = p_1 \cdots p_r$.

(ii) Si $q_1, \ldots, q_s \in A$ es una colección finita de elementos irreducibles tales que $a = q_1 \cdots q_s$, entonces $r = s$ y existe una permutación σ de los índices $1, \ldots, r$ tal que q_i y $p_{\sigma(i)}$ son asociados para cada $i = 1, \ldots, r$.

Proposición I.10 *Dados elementos $a_1, \ldots, a_r$ en un* DFU *existe su máximo común divisor* $\mathrm{mcd}_A(a_1, \ldots, a_r)$.

Demostración. Como A es un DFU los divisores irreducibles comunes a $a_1, \ldots, a_r$ forman, (salvo producto por unidades) un conjunto finito. Denotemos $p_1, \ldots, p_k$ dichos factores irreducibles comunes y escribimos

$$a_i := \prod_{j=1}^{k} p_j^{\gamma_{ij}} \cdot b_i, \text{ donde } b_i \in A \text{ y cada } \gamma_{ij} \in \mathbb{Z}, \text{ es positivo.}$$

Para cada $j = 1, \ldots, k$ sea $\gamma_j := \mín\{\gamma_{ij} : i = 1, \ldots, r\}$. Se comprueba inmediatamente que $d := \prod_{j=1}^{k} p_j^{\gamma_j}$ es un máximo común divisor de $a_1, \ldots, a_r$ en A. □

Definiciones I.11 Sean A un DFU y $f := \sum_{i=0}^{d} a_i \mathtt{t}^i \in A[\mathtt{t}]$ no nulo. Se llama *contenido* de f en A a $\mathtt{c}_A(f) := \mathrm{mcd}_A(a_0, \ldots, a_d)$. Se dice que f es *primitivo* en A si $\mathtt{c}_A(f) = 1$.

Observaciones I.12 Sean A un DFU y $f := \sum_{i=0}^{d} a_i \mathtt{t}^i \in A[\mathtt{t}]$ un polinomio no nulo.

(1) Existe un polinomio primitivo $f_1 \in A[\mathtt{t}]$ tal que $f = \mathtt{c}_A(f) f_1$.

En efecto, cada a_k es múltiplo de $\mathtt{c}_A(f)$ en A, luego existe $b_k \in A$ tal que $a_k = \mathtt{c}_A(f) b_k$. El polinomio

$$f_1(\mathtt{t}) := \sum_{k=0}^{n} b_k \mathtt{t}^k \in A[\mathtt{t}]$$

cumple la igualdad $f = \mathtt{c}_A(f) f_1$, y queda ver que f_1 es primitivo. Ahora bien,

$$\begin{aligned} \mathtt{c}_A(f) = \mathrm{mcd}_A\left(a_0, \ldots, a_n\right) &= \mathrm{mcd}_A\left(\mathtt{c}_A(f) b_0, \ldots, \mathtt{c}_A(f) b_n\right) \\ &= \mathtt{c}_A(f)\, \mathrm{mcd}_A\left(b_0, \ldots, b_n\right) = \mathtt{c}_A(f) \mathtt{c}_A(f_1), \end{aligned}$$

y como A es un dominio se concluye que $\mathtt{c}_A(f_1) = 1$.

(2) Por el mismo argumento, $\mathtt{c}_A(bf) = b\mathtt{c}_A(f)$ para cada $b \in A$.

(3) Sean $a, b \in A \setminus \{0\}$ y $f, g \in A[\mathtt{t}]$ polinomios primitivos tales que $af = bg$. Entonces, salvo producto por unidades, se puede suponer que $a = b$ y $f = g$.

En efecto, por el apartado anterior, y puesto que f y g son primitivos, se tiene

$$a = a\mathtt{c}_A(f) = \mathtt{c}_A(af) = \mathtt{c}_A(bg) = b\mathtt{c}_A(g) = b.$$

Además, $a(f - g) = af - bg = 0$. Como $A[\mathtt{t}]$ es un dominio y $a \neq 0$ deducimos que $f = g$.

(4) Todo polinomio irreducible $f \in A[\mathtt{t}]$ es primitivo, pues en caso contrario tanto $\mathtt{c}_A(f)$ como f_1 son no unidades en $A[\mathtt{t}]$ y cumplen $f = \mathtt{c}_A(f) f_1$.

(5) Si A es un cuerpo, entonces todo polinomio no nulo $f \in A[\mathtt{t}]$ es primitivo en $A[\mathtt{t}]$, pues todos los elementos no nulos de A son unidades en A.

(6) Sean $a_0, b_0, \ldots, a_n, b_n \in A$ tales que cada $b_k \neq 0$ y

$$g(\mathtt{t}) = \sum_{k=0}^{n} \left(\frac{a_k}{b_k}\right) \mathtt{t}^k \in K[\mathtt{t}],$$

donde K es el cuerpo de fracciones de A. Sea $b := b_0 \cdots b_n$. Entonces $bg \in A[\mathtt{t}]$.

En efecto, cada $b_k | b$, luego existe $c_k \in A$ tal que $b = b_k c_k$, y por tanto,

$$bg(\mathtt{t}) = \sum_{k=0}^{n} \left(\frac{ba_k}{b_k}\right) \mathtt{t}^k = \sum_{k=0}^{n} (a_k c_k) \mathtt{t}^k \in A[\mathtt{t}].$$

Comentario I.13 Fijado $f \in A[\mathtt{t}]$, donde A es un DFU, y si $K := \mathrm{qf}(A)$, Gauss estudió la relación entre la irreducibilidad de f como elemento de $A[\mathtt{t}]$ y como elemento de $K[\mathtt{t}]$. Recordamos a continuación este resultado.

Lema I.14 *Sean A un* DFU *y $f, g \in A[\mathtt{t}]$ no nulos. Entonces $\mathtt{c}_A(fg) = \mathtt{c}_A(f)\mathtt{c}_A(g)$. En particular, el producto de polinomios primitivos en $A[\mathtt{t}]$ es primitivo en $A[\mathtt{t}]$.*

Demostración. Escribimos $f = \mathtt{c}_A(f)f_1$ y $g = \mathtt{c}_A(g)g_1$ donde $f_1, g_1 \in A[\mathtt{t}]$ son polinomios primitivos. Como $fg = \mathtt{c}_A(f)\mathtt{c}_A(g)f_1g_1$, se deduce de I.12 (2) que

$$\mathtt{c}_A(fg) = \mathtt{c}_A(f)\mathtt{c}_A(g)\mathtt{c}_A(f_1g_1),$$

luego basta ver que f_1g_1 es un polinomio primitivo. Si no lo fuese, el ideal generado en $A[\mathtt{t}]$ por los coeficientes de f_1g_1 sería propio, luego existiría un ideal maximal $\mathfrak{m}$ de A que los contendría. Consideremos el cuerpo $E := A/\mathfrak{m}$ y el homomorfismo

$$\pi : A[\mathtt{t}] \to E[\mathtt{t}], \sum_{i=0}^{d} a_i\mathtt{t}^i \mapsto \sum_{i=0}^{d}(a_i + \mathfrak{m})\mathtt{t}^i.$$

Se tiene $\pi(f_1)\pi(g_1) = \pi(f_1g_1) = 0$ y, como $E[\mathtt{t}]$ es un dominio de integridad, podemos suponer que $\pi(f_1) = 0$, esto es, cada $a_i \in \mathfrak{m}$, por lo que $\mathtt{c}_A(f_1) \neq 1$, esto es, f_1 no es primitivo, que es una contradicción. □

Corolario I.15 *Sean A un* DFU*, K su cuerpo de fracciones y $f \in A[\mathtt{t}]$ con* $\deg(f) \geq 1$*. Entonces f es irreducible en $A[\mathtt{t}]$ si y sólo si es irreducible en $K[\mathtt{t}]$ y $\mathtt{c}_A(f) = 1$.*

Demostración. Supongamos en primer lugar que f es irreducible en $A[\mathtt{t}]$, lo que por la Observación I.12(4) implica que es primitivo. Para demostrar que f es irreducible en $K[\mathtt{t}]$, sean $g, h \in K[\mathtt{t}]$ tales que $f = gh$. Hemos de comprobar que g o h es una unidad en $K[\mathtt{t}]$. Se deduce de las Observaciones I.12 (1) y (6) que existen $a, b \in A \setminus \{0\}$ y polinomios primitivos $g_1, h_1 \in A[\mathtt{t}]$ tales que $ag, bh \in A[\mathtt{t}]$, $ag = \mathtt{c}_A(ag)g_1$ y $bh = \mathtt{c}_A(bh)h_1$. Así,

$$abf = abgh = (ag)(bh) = \mathtt{c}_A(ag)g_1\mathtt{c}_A(bh)h_1 = \mathtt{c}_A(ag)\mathtt{c}_A(bh)g_1h_1,$$

y como f es primitivo por hipótesis y g_1h_1 lo es por el Lema I.14, se deduce de la Observación I.12(3) que $f = g_1h_1$. Como f es irreducible en $A[\mathtt{t}]$, esta igualdad implica que g_1 o h_1 es unidad en $A[\mathtt{t}]$, y por tanto en A. Suponemos, por ejemplo, que g_1 es unidad en A. Entonces $g = \mathtt{c}_A(ag)g_1/a$ es unidad en K, y por tanto en $K[\mathtt{t}]$, como queríamos demostrar.

Suponemos ahora que f es irreducible en $K[\mathtt{t}]$ y $\mathtt{c}_A(f) = 1$. Sean $g, h \in A[\mathtt{t}]$ con $f = gh$. Es suficiente comprobar que g o h es unidad en $A[\mathtt{t}]$. La irreducibilidad de f en $K[\mathtt{t}]$ asegura que, por ejemplo, $g \in \mathcal{U}(K[\mathtt{t}]) = K \setminus \{0\}$. En consecuencia, $\deg(g) = 0$, por lo que $g \in A \setminus \{0\}$. Además, $1 = \mathtt{c}_A(f) = \mathtt{c}_A(gh) = g\mathtt{c}_A(h)$, luego $g \in \mathcal{U}(A) = \mathcal{U}(A[\mathtt{t}])$, como queríamos probar. □

El Corolario anterior pone de manifiesto que estudiar la irreducibilidad de $f \in A[\mathtt{t}]$ en $A[\mathtt{t}]$ o en $K[\mathtt{t}]$ son cuestiones esencialmente iguales, aunque no idénticas. Por ejemplo, $f(\mathtt{t}) := 2\mathtt{t}$ es reducible en $\mathbb{Z}[\mathtt{t}]$ pero irreducible en $\mathbb{Q}[\mathtt{t}]$ ya que 2 es unidad en $\mathbb{Q}$ pero no en $\mathbb{Z}$. Para evitar esta patología siempre trataremos en lo sucesivo con polinomios primitivos.

Para terminar esta sección señalemos que una importante consecuencia del Corolario I.15 es el siguiente resultado, que no demostraremos pero emplearemos varias veces a lo largo del trabajo.

Teorema I.16 *Sea A un dominio. Entonces, A es un* DFU *si y sólo si $A[\mathtt{t}]$ es un* DFU*.*

CAPÍTULO II

Criterios modulares

Una estrategia útil en Álgebra consiste en estudiar las propiedades de un elemento a de un anillo A analizando las *reducciones modulares* de a, es decir, las imágenes de a vía las proyecciones canónicas $A \to A/\mathfrak{a}$ cuando $\mathfrak{a}$ recorre una clase distinguida de ideales de A. La siguiente proposición y el Criterio modular II.2 son ejemplos de este modo de proceder.

Proposición II.1 *Sean A un* DFU*, $f := \sum_{k=0}^{d} a_k \mathtt{t}^k \in A[\mathtt{t}]$ un polinomio primitivo en $A[\mathtt{t}]$ de grado $d \geq 1$ y $\mathfrak{a}$ un ideal de A tal que $a_d \notin \mathfrak{a}$. Sea $B := A/\mathfrak{a}$ y consideramos el epimorfismo de anillos*

$$\varphi : A[\mathtt{t}] \to B[\mathtt{t}],\ \sum_{j=0}^{m} b_j \mathtt{t}^j \mapsto \sum_{j=0}^{m} (b_j + \mathfrak{a})\mathtt{t}^j.$$

Si $\varphi(f)$ no es producto de dos polinomios de $B[\mathtt{t}]$ de grado ≥ 1 cuya suma de grados es igual a $\deg(f)$, entonces f es irreducible en $A[\mathtt{t}]$.

Demostración. Si f fuese reducible en $A[\mathtt{t}]$ existirían $g, h \in A[\mathtt{t}]$ de grados respectivos $n, m \geq 1$ tales que $f = gh$ y $n + m = d$. Nótese que $\ell(g)\ell(h) = \ell(f) = a_r \notin \mathfrak{a}$, luego $\ell(g), \ell(h) \notin \mathfrak{a}$, lo que implica que $\varphi(g)$ y $\varphi(h)$ son polinomios en $B[\mathtt{t}]$ de grados $n, m \geq 1$ respectivamente, tales que $\varphi(f) = \varphi(g)\varphi(h)$, que es una contradicción. □

Corolario II.2 (Criterio modular) *Sean A un* DFU*, $f(\mathtt{t}) := \sum_{k=0}^{d} a_k \mathtt{t}^k \in A[\mathtt{t}]$ un polinomio primitivo de grado $d \geq 1$ y $\mathfrak{p}$ un ideal primo de A tal que $a_d \notin \mathfrak{p}$. Denotemos $B := A/\mathfrak{p}$ y consideramos el epimorfismo de anillos*

$$\varphi : A[\mathtt{t}] \to B[\mathtt{t}],\ \sum_{j=0}^{m} b_j \mathtt{t}^j \mapsto \sum_{j=0}^{m} (b_j + \mathfrak{p})\mathtt{t}^j.$$

Si f es reducible en $A[\mathtt{t}]$, entonces $\varphi(f)$ es reducible en $B[\mathtt{t}]$. Se dice que $\varphi(f)$ es la *reducción* de f módulo $\mathfrak{p}$.

Demostración. Como $\mathfrak{p}$ es un ideal primo el anillo B es un dominio luego también lo es $B[\mathtt{t}]$. Como f es primitivo y reducible se escribe como producto $f = gh$ para ciertos polinomios $g, h \in A[\mathtt{t}]$ de grado mayor o igual que 1. En particular, $\ell(g) \cdot \ell(h) = a_d \in A \setminus \mathfrak{p}$, luego $\ell(g) \in A \setminus \mathfrak{p}$ y $\ell(h) \in A \setminus \mathfrak{p}$. Por tanto $\varphi(f)$ es reducible en $B[\mathtt{t}]$por ser producto de dos polinomios de $B[\mathtt{t}]$ de grado ≥ 1:

$$\varphi(f) = \varphi(g) \cdot \varphi(h) \quad \text{y} \quad \deg(\varphi(g)) = \deg(g) \geq 1, \quad \deg(\varphi(h)) = \deg(h) \geq 1. \qquad \square$$

Ejemplo II.3 Veamos que el polinomio $f(\mathtt{t}) := \mathtt{t}^5 - \mathtt{t} + 1$ es irreducible en $\mathbb{Z}[\mathtt{t}]$ viendo que su reducción $\mathsf{mod}\, 5$, que por abuso también denotaremos f, lo es en $\mathbb{Z}_5[\mathtt{t}]$. El polinomio f carece de raíces en $\mathbb{Z}_5$ pues, por el Pequeño Teorema de Fermat, $z^5 \equiv z \ \mathsf{mod}\ 5$ para cada $z \in \mathbb{Z}$, luego $f(x) = 1$ para cada $x \in \mathbb{Z}_5$. Así, si f fuese reducible en $\mathbb{Z}_5[\mathtt{t}]$, y puesto que carece de término en $\mathtt{t}^4$, se escribiría como producto

$$\mathtt{t}^5 - \mathtt{t} + 1 = (\mathtt{t}^3 + a\mathtt{t}^2 + b\mathtt{t} + c)(\mathtt{t}^2 - a\mathtt{t} + d)$$

para ciertos $a, b, c, d \in \mathbb{Z}_5$. Igualando los coeficientes de ambos miembros se obtiene

$$\begin{cases} b & - & a^2 & + & d & = & 0 \\ a(d-b) & + & c & & & = & 0 \\ bd & - & ac & & & = & -1 \\ cd & & & & & = & 1 \end{cases}$$

Al sustituir el valor $b = a^2 - d$ en la segunda ecuación resulta $c = a(a^2 - 2d)$. Reemplazamos estos dos valores en la tercera ecuación, y resulta

$$(a^2 - d)d = a^2(a^2 - 2d) - 1, \tag{II.1}$$

por lo que $d^2 - 3a^2d + a^4 - 1 = 0$. Como trabajamos en $\mathbb{Z}_5$ esta igualdad equivale a

$$0 = d^2 + 2a^2d + a^4 - 1 = (d + a^2)^2 - 1,$$

luego $d + a^2 = \varepsilon := \pm 1$. Al sustituir el valor $d = \varepsilon - a^2$ en la cuarta ecuación del sistema anterior, y recordando que $a^5 = a$, se obtiene una contradicción:

$$\begin{aligned} 1 = cd = ad(a^2 - 2d) &= a(\varepsilon - a^2)(3a^2 - 2\varepsilon) = a(\varepsilon - a^2)(3a^2 + 3\varepsilon) \\ &= 3a(\varepsilon - a^2)(\varepsilon + a^2) = 3a(1 - a^4) = 3(a - a^5) = 0. \end{aligned}$$

Ejemplo II.4 El polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 10\mathtt{t}^2 + 1 \in \mathbb{Z}[\mathtt{t}]$ es irreducible en $\mathbb{Z}[\mathtt{t}]$. Para verlo aplicamos la Proposición II.1 tomando $\mathfrak{a} := 9\mathbb{Z}$. En efecto, por ser mónico f es primitivo y su coeficiente director no pertenece a $\mathfrak{a}$. Además, su reducción $\overline{f}_9 \ \mathsf{mod}\ 9$ no es divisible por ningún polinomio en $\mathbb{Z}_9[\mathtt{t}]$ de grado 1, pues carece de raíces en $\mathbb{Z}_9$:

$$\begin{aligned} &\overline{f}_9(0) = \overline{f}_9(1) = \overline{f}_9(-1) = \overline{f}_9(3) = \overline{f}_9(-3) = [1]_9; \\ &\overline{f}_9(2) = \overline{f}_9(-2) = [4]_9 \quad \text{y} \quad \overline{f}_9(4) = \overline{f}_9(-4) = [7]_9. \end{aligned}$$

Veamos que $\overline{f}_9$ tampoco es producto de dos polinomios de grado 2 en $\mathbb{Z}_9[\mathtt{t}]$. En caso contrario podemos suponer, por la Observación I.4, que ambos factores son mónicos, por serlo $\overline{f}_9$, así que existirían números enteros a, b, c, d tales que

$$\overline{f}_9 = (\mathtt{t}^2 + [a]_9\mathtt{t} + [b]_9) \cdot (\mathtt{t}^2 + [c]_9\mathtt{t} + [d]_9). \tag{II.2}$$

Igualando coeficientes en ambos miembros resultan las siguientes congruencias $\mathsf{mod}\ 9$:

$$bd \equiv 1, \ \ bc + ad \equiv 0, \ \ b + ac + d \equiv -10 \equiv -1 \ \text{ y } \ a + c \equiv 0. \tag{II.3}$$

Despejando $c \equiv -a$ en la última ecuación y sustituyendo este valor en la tercera resulta

$$bd \equiv 1 \quad \text{y} \quad a^2 \equiv b + d + 1.$$

Las unidades de $\mathbb{Z}_9$ son $[1]_9$, $[2]_9$, $[4]_9$, $[5]_9$, $[7]_9$, $[8]_9$, y cumplen

$$[1]_9^2 = [2]_9 \cdot [5]_9 = [4]_9 \cdot [7]_9 = [8]_9^2 = [1]_9.$$

Por otro lado, los cuadrados en $\mathbb{Z}_9$ son $[0]_9$, $[1]_9$, $[4]_9$, $[7]_9$. Distinguimos casos según los valores del par (b, d), teniendo en cuenta que $[b]_9 \cdot [d]_9 = [1]_9$.

(i) Si $b \equiv d \equiv 1$, entonces $a^2 \equiv b + d + 1 \equiv 3$, que es imposible.

(ii) Si $b \equiv 2$, $d \equiv 5$ (o viceversa), entonces $a^2 \equiv b + d + 1 \equiv 8$, que también es imposible.

(iii) Si $b \equiv 4$, $d \equiv 7$ (o viceversa), entonces $a^2 \equiv b + d + 1 \equiv 12 \equiv 3$, imposible de nuevo.

(iv) Si $b \equiv d \equiv 8$, entonces $a^2 \equiv b + d + 1 \equiv 17 \equiv 8$, que es imposible una vez más.

Esto prueba que f es irreducible en $\mathbb{Z}[\mathtt{t}]$.

El siguiente resultado tiene dos lecturas. En ocasiones permite averiguar los grados de los factores irreducibles de un polinomio reducible en $\mathbb{Z}[\mathtt{t}]$. En otras, como veremos en el ejemplo II.6, sirve para decidir que un polinomio con coeficientes enteros es irreducible.

Proposición II.5 *Sean $f \in \mathbb{Z}[\mathtt{t}]$ un polinomio mónico y $\overline{f} \in \mathbb{Z}_p[\mathtt{t}]$ la reducción de f mod p para cierto primo p. Supongamos que existen g_1, g_2 en $\mathbb{Z}_p[\mathtt{t}]$ de grados d_1 y d_2 irreducibles y distintos tales que $\overline{f} = g_1 \cdot g_2$. Entonces, si f es reducible en $\mathbb{Z}[\mathtt{t}]$, es producto de dos polinomios irreducibles en $\mathbb{Z}[\mathtt{t}]$ de grados d_1 y d_2, respectivamente.*

Demostración. Puesto que $\mathbb{Z}[\mathtt{t}]$ es un DFU y estamos suponiendo que f es mónico y reducible en $\mathbb{Z}[\mathtt{t}]$, existen polinomios mónicos $f_1, f_2 \in \mathbb{Z}[\mathtt{t}]$ de grado al menos 1 tales que $f = f_1 f_2$. Al reducir mod p obtenemos $g_1 g_2 = \overline{f} = \overline{f}_1 \overline{f}_2$ y, puesto que f_i es mónico, $\deg(f_i) = \deg(\overline{f}_i)$ para $i = 1, 2$. Como g_1 divide al producto $\overline{f}_1 \overline{f}_2$ y es irreducible en $\mathbb{Z}_p[\mathtt{t}]$, que es un DFU, podemos suponer, sin pérdida de generalidad, que $g_1 | \overline{f}_1$. Si g_2 también dividiese a $\overline{f}_1$ entonces $g_1 g_2 | \overline{f}_1$, y por tanto, como $\deg(f) = \deg(\overline{f})$ ya que f es mónico,

$$\begin{aligned} \deg(f) = \deg(f_1) + \deg(f_2) = \deg(\overline{f}_1) + \deg(\overline{f}_2) > \deg(\overline{f}_1) \geq \deg(g_1 g_2) \\ = \deg(g_1) + \deg(g_2) = \deg(\overline{f}) = \deg(f), \end{aligned}$$

que es imposible. Así, g_2 es irreducible y divide a $\overline{f}_1 \overline{f}_2$ pero no divide a $\overline{f}_1$, luego divide a $\overline{f}_2$. Por tanto, existen polinomios $q_1, q_2 \in \mathbb{Z}_p[\mathtt{t}]$ tales que $\overline{f}_1 = g_1 q_1$ y $\overline{f}_2 = g_2 q_2$. Pero

$$\begin{aligned} \deg(q_1) + \deg(q_2) = \deg(\overline{f}_1) - \deg(g_1) + \deg(\overline{f}_2) - \deg(g_2) = \deg(\overline{f}_1) + \deg(\overline{f}_2) \\ - \deg(g_1) - \deg(g_2) = \deg(\overline{f}_1 \overline{f}_2) - \deg(g_1 g_2) = \deg(\overline{f}) - \deg(\overline{f}) = 0, \end{aligned}$$

luego $\deg(q_1) = \deg(q_2) = 0$. Así, $\deg(f_i) = \deg(\overline{f}_i) = \deg(g_i) = d_i$ para $i = 1, 2$ y $f = f_1 f_2$. Además, la irreducibilidad de cada $\overline{f}_i$ implica, por el Corolario II.2, la de f_i, lo que concluye la prueba. □

Ejemplo II.6 Vamos a demostrar, empleando la observación anterior, que el polinomio

$$f(\mathtt{t}) = \mathtt{t}^5 - 6\mathtt{t}^4 + 5\mathtt{t}^2 - \mathtt{t} + 2 \in \mathbb{Z}[\mathtt{t}]$$

es irreducible en $\mathbb{Z}[\mathtt{t}]$. Su reducción $\mathsf{mod}\ 2$ es

$$\overline{f} = \mathtt{t}^5 + \mathtt{t}^2 + \mathtt{t} = \mathtt{t}(\mathtt{t}^4 + \mathtt{t} + 1).$$

El factor $\mathtt{t}$ es irreducible en $\mathbb{Z}_2[\mathtt{t}]$, y también lo es $\mathtt{t}^4 + \mathtt{t} + 1$. En efecto, es evidente que no tiene raíces en $\mathbb{Z}_2$, luego si fuese reducible sería producto de dos polinomios irreducibles de grado 2. El único polinomio irreducible de grado 2 de $\mathbb{Z}_2[\mathtt{t}]$ es $\mathtt{t}^2 + \mathtt{t} + 1$, así que

$$\mathtt{t}^4 + \mathtt{t} + 1 = (\mathtt{t}^2 + \mathtt{t} + 1)^2 = \mathtt{t}^4 + \mathtt{t}^2 + 1,$$

y esto es falso. Se deduce de la Proposición II.5 que si f es reducible en $\mathbb{Z}[\mathtt{t}]$ entonces es producto de un polinomio de grado 1 por otro de grado 4. En particular f tendría una raíz racional, luego entera, pues es mónico, que necesariamente es un divisor de 2. Sin embargo,

$$f(1) = f(-1) = 1, \quad f(2) = -44 \quad \text{y} \quad f(-2) = -104.$$

Concluimos que f es irreducible en $\mathbb{Z}[\mathtt{t}]$, y por tanto también lo es en $\mathbb{Q}[\mathtt{t}]$.

La siguiente aplicación de la Proposición II.5 muestra otro modo de demostrar la irreducibilidad de algunos polinomios.

Ejemplo II.7 Veamos que $f(\mathtt{t}) := \mathtt{t}^5 - 6\mathtt{t}^4 + 5\mathtt{t}^2 - \mathtt{t} + 2$ es irreducible en $\mathbb{Z}[\mathtt{t}]$. Su reducción $\mathsf{mod}\, 2$ es

$$\overline{f}_2(\mathtt{t}) = \mathtt{t}^5 + \mathtt{t}^2 + \mathtt{t} = \mathtt{t} \cdot (\mathtt{t}^4 + \mathtt{t} + 1),$$

y éstos son los factores irreducibles de $\overline{f}$ en $\mathbb{Z}_2[\mathtt{t}]$. En efecto, el segundo factor carece de raíces en $\mathbb{Z}_2$, luego si fuese reducible en $\mathbb{Z}_2[\mathtt{t}]$ existiría $a \in \{0, 1\}$ tal que

$$\mathtt{t}^4 + \mathtt{t} + 1 = (\mathtt{t}^2 + a\mathtt{t} + 1)(\mathtt{t}^2 + a\mathtt{t} + 1) = \mathtt{t}^4 + a^2\mathtt{t}^2 + 1,$$

lo cual es falso. Así, si f fuese reducible en $\mathbb{Z}[\mathtt{t}]$ sería, en virtud de la Proposición II.5, producto de dos polinomios irreducibles en $\mathbb{Z}[\mathtt{t}]$ de grados 1 y 4.

Por otro lado, la reducción de f $\mathsf{mod}\, 3$ es

$$\overline{f}_3(\mathtt{t}) = \mathtt{t}^5 + 2\mathtt{t}^2 + 2\mathtt{t} + 2 = (\mathtt{t}^2 + 1) \cdot (\mathtt{t}^3 + 2\mathtt{t} + 2),$$

y ambos factores son irreducibles en $\mathbb{Z}_3[\mathtt{t}]$ porque su grado es ≤ 3 y carecen de raíces en $\mathbb{Z}_3$. Empleando de nuevo la Proposición II.5 se deduce que si f fuese reducible en $\mathbb{Z}[\mathtt{t}]$ sería producto de dos polinomios irreducibles en $\mathbb{Z}[\mathtt{t}]$ de grados 2 y 3, lo que contradice lo probado con anterioridad ya que la factorización de f en producto de polinomios irreducibles en $\mathbb{Z}[\mathtt{t}]$ es única.

CAPÍTULO III

Criterios tipo Eisenstein

El objetivo fundamental de esta sección es presentar un resultado original, Lema III.2, que generaliza el clásico Criterio de Eisenstein y permite deducir un nuevo criterio de irreduciblidad de polinomios. Aprovechamos para exponer la versión del Criterio de Eisenstein en la que el orden de los coeficientes es el inverso del usual y el Criterio de Netto.

Lema III.1 *Sean A un dominio y $f(\mathtt{t}) := \sum_{k=0}^{d} a_k \mathtt{t}^k \in A[\mathtt{t}]$ tal que a_0 y a_d no son nulos. Entonces f es irreducible en $A[\mathtt{t}]$ si y sólo si es irreducible en $A[\mathtt{t}]$ el polinomio*

$$\widehat{f}(\mathtt{t}) := \sum_{k=0}^{d} a_k \mathtt{t}^{d-k} = \mathtt{t}^{\deg(f)} f(1/\mathtt{t}).$$

Demostración. Como $\widehat{\widehat{f}} = f$ es suficiente demostrar que si f es reducible en $A[\mathtt{t}]$ entonces también $\widehat{f}$ lo es. Sean $h_1, h_2 \in A[\mathtt{t}] \setminus \{0\}$ no unidades tales que $f = h_1 h_2$. Los polinomios $\widehat{h_i}(\mathtt{t}) := \mathtt{t}^{\deg(h_i)} h_i(1/\mathtt{t}) \in A[\mathtt{t}] \setminus \{0\}$ no son unidades y $\widehat{f} = \widehat{h_1}\widehat{h_2}$, lo que prueba la reducibilidad de $\widehat{f}$ en $A[\mathtt{t}]$. □

Lema III.2 *Sean A un* DFU *y $f(\mathtt{t}) := \sum_{i=0}^{n} a_i \mathtt{t}^i \in A[\mathtt{t}]$ un polinomio primitivo. Supongamos que existen un elemento irreducible $p \in A$ y un número entero $0 \leq k < n$ tales que p divide a los coeficientes $a_0, \ldots, a_k$ y p^2 no divide a a_0. Entonces f tiene algún factor irreducible en $A[\mathtt{t}]$ de grado mayor o igual que $k+1$.*

Demostración. Sea $f := f_1 \cdots f_\ell$ la factorización de f como producto de factores irreducibles en $A[\mathtt{t}]$ y suponemos que $\deg(f_i) \leq k$ para $i = 1, \ldots, \ell$. Por el Lema I.14,

$$1 = \mathtt{c}_A(f) = \mathtt{c}_A(f_1) \cdots \mathtt{c}_A(f_\ell),$$

luego los factores irreducibles de f en $A[\mathtt{t}]$ son primitivos. Como $a_0 = f(0) = f_1(0) \cdots f_\ell(0)$ y $p | a_0$ pero $p^2 \nmid a_0$ podemos suponer que $p | f_1(0)$ pero $p \nmid f_i(0)$ para $i = 2, \ldots, \ell$. Denotamos

$$g(\mathtt{t}) := f_1(\mathtt{t}) := \sum_{i=0}^{m} b_i \mathtt{t}^i \quad \text{y} \quad h(\mathtt{t}) := f_2(\mathtt{t}) \cdots f_\ell(\mathtt{t}) := \sum_{j=0}^{r} c_j \mathtt{t}^j,$$

donde $m := \deg(g) \leq k$. Nótese que $p | b_0$ pero $p \nmid c_0 = f_2(0) \cdots f_\ell(0)$. Como g es primitivo, existe un índice s con $1 \leq s \leq m$ tal que $p | b_i$ para $0 \leq i < s$ y $p \nmid b_s$. Como $s \leq m \leq k$, el primo p divide a $a_s = b_0 c_s + \cdots + b_{s-1} c_1 + b_s c_0$, luego $p | b_s c_0$ y esto es falso porque p no divide ni a b_s ni a c_0. Por tanto, alguno de los factores irreducibles de f tiene grado mayor o igual que $k+1$. □

Corolario III.3 (Criterio de Eisenstein) *Sean A un* DFU, *p un elemento irreducible de A y $f(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i \in A[\mathtt{t}]$ un polinomio primitivo. Supongamos que p divide a $a_0, \ldots, a_{d-1}$ y p^2 no divide a a_0. Entonces f es irreducible en $A[\mathtt{t}]$.*

Demostración. Del Lema anterior con $k := d-1$ se deduce que f tiene un factor irreducible en $A[\mathtt{t}]$ cuyo grado es mayor o igual que $k+1 = d = \deg(f)$. Como f es primitivo, es irreducible en $A[\mathtt{t}]$. □

Ejemplo III.4 El polinomio $f(\mathtt{t}) := \mathtt{t}^7 + 3\mathtt{t}^4 - 6\mathtt{t}^3 + 12\mathtt{t} + 15$ es irreducible en $\mathbb{Z}[\mathtt{t}]$ en virtud del Criterio de Eisenstein aplicado con el primo $p := 3$.

Corolario III.5 *Sean A un* DFU *y $f(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i \in A[\mathtt{t}]$ primitivo de grado d. Supongamos que f no tiene raíces en $K := \mathrm{qf}(A)$ y que existe un elemento irreducible p en A que divide a $a_0, \ldots, a_{d-2}$ pero p^2 no divide a a_0. Entonces f es irreducible en $A[\mathtt{t}]$.*

Demostración. Aplicando el Lema III.2 con $k := d-2$ el polinomio f tiene algún factor irreducible en $A[\mathtt{t}]$ de grado mayor o igual que $k+1 = d-1$. Esto implica, por ser f primitivo que, o bien es irreducible en $A[\mathtt{t}]$ y hemos terminado, o bien $f(\mathtt{t}) := (a\mathtt{t}-b)\cdot g(\mathtt{t})$ para ciertos $a, b \in A$ tales que $a \neq 0$ y $g \in A[\mathtt{t}]$. Esto último no puede darse porque implicaría que $u := \frac{b}{a} \in K$ es raíz de f, contra la hipótesis. □

Ejemplo III.6 Aplicamos el Corolario anterior con el primo $p := 5$ para demostrar que el polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 3\mathtt{t}^3 + 5\mathtt{t}^2 + 10$ es irreducible en $\mathbb{Z}[\mathtt{t}]$. Por un lado 5 divide a todos los coeficientes de f salvo a los que acompañan a $\mathtt{t}^4$ y $\mathtt{t}^3$. Además, $5^2 = 25$ no divide a 10 y f es primitivo. Como $f(0) = 10 = 5 \cdot 2$, las posibles raíces racionales de f pertenecen al conjunto $\{-1,\ 1,\ -2,\ 2,\ -5,\ 5,\ -10,\ 10\}$. Pero

$$\begin{aligned} f(-10) = 13510,\ \ f(10) = 7510,\ \ f(-5) = 1135\ \ f(5) = 385,\\ f(-2) = 70,\ \ f(2) = 22\ \ f(-1) = 19,\ \ f(1) = 13, \end{aligned}$$

luego f no tiene raíces en $\mathbb{Q}$, y se deduce del Corolario III.5 que es irreducible en $\mathbb{Z}[\mathtt{t}]$.

Ejemplos III.7 (1) Sean p un primo positivo y $1 \leq k \leq p-1$. Entonces, el número combinatorio $c_k := \binom{p}{k}$ es múltiplo de p. En efecto, $c_k \cdot k! \cdot (p-k)! = p! \in p\mathbb{Z}$. La primalidad de p garantiza que no divide a ningún producto de números enteros positivos menores que p, luego $p \nmid k!$ y $p \nmid (p-k)!$. Como p es primo y divide a $c_k \cdot k! \cdot (p-k)!$ se deduce que $p | c_k$.

(2) Para cada número primo p se llama p-ésimo *polinomio ciclotómico* al polinomio

$$\Phi_p(\mathtt{t}) := \sum_{k=0}^{p-1} \mathtt{t}^k \in \mathbb{Z}[\mathtt{t}].$$

El polinomio Φ_p es irreducible en $\mathbb{Z}[\mathtt{t}]$. En efecto, por la Proposición I.7 basta demostrar la irreducibilidad en $\mathbb{Z}[\mathtt{t}]$ del polinomio $f(\mathtt{t}) := \Phi_p(\mathtt{t}+1)$. Como $(\mathtt{t}-1)\Phi_p(\mathtt{t}) = \mathtt{t}^p - 1$ se tiene $\mathtt{t}\Phi_p(\mathtt{t}+1) = (\mathtt{t}+1)^p - 1$, luego

$$\mathtt{t} f(\mathtt{t}) = \mathtt{t}\Phi_p(\mathtt{t}+1) = (\mathtt{t}+1)^p - 1 = \sum_{k=0}^{p} \binom{p}{k} \mathtt{t}^k - 1 = \mathtt{t} \sum_{k=1}^{p} \binom{p}{k} \mathtt{t}^{k-1},$$

y simplificando el factor $\mathtt{t}$ resulta $f(\mathtt{t}) = \sum_{k=1}^{p} \binom{p}{k} \mathtt{t}^{k-1}$. Por el apartado (1) cada coeficiente $\binom{p}{k}$ con $k \neq p$ es múltiplo de p y p^2 no divide a $p = \binom{p}{1}$ luego, por el Criterio de Eisenstein, f es irreducible en $\mathbb{Z}[\mathtt{t}]$.

(3) Veamos que $f(\mathtt{t}) := 3\mathtt{t}^5 - 5\mathtt{t}^4 + 15\mathtt{t}^3 + 5\mathtt{t} + 16$ es irreducible en $\mathbb{Z}[\mathtt{t}]$. Buscamos un entero a de modo que podamos aplicar el Criterio de Eisenstein para el primo 5 al polinomio trasladado $h_a(\mathtt{t}) := f(\mathtt{t} + a)$. Como los números combinatorios $\binom{5}{k}$ son múltiplos de 5 en virtud de lo probado en el apartado (1), deducimos que 5 divide a todos los coeficientes del polinomio h_a distintos del término independiente y de su coeficiente director, que vale 1. Por tanto, para aplicar el Criterio de Eisenstein basta exigir que su término independiente

$$h_a(0) = f(a) := 3a^5 - 5a^4 + 15a^3 + 5a + 16$$

sea múltiplo de 5 pero no de 25. Por el Pequeño Teorema de Fermat, $a^5 \equiv a \bmod 5$, luego $f(a) \equiv 3a + 1 \bmod 5$, lo que induce a elegir $a = 3$. Como $3^3 \equiv 2 \bmod 25$,

$$f(3) = 3^6 - 5 \cdot 3^4 + 5 \cdot 3^4 + 31 \equiv (3^3)^2 + 6 \bmod 25 \equiv 10 \bmod 25 \neq 0 \bmod 25.$$

Proposición III.8 (Criterio de Eisenstein modificado) *Sean A un* DFU *y el polinomio primitivo $f(\mathtt{t}) := \sum_{k=0}^{d} a_k \mathtt{t}^k \in A[\mathtt{t}]$ de grado d. Supongamos que $a_0 \neq 0$ y que existe un elemento irreducible $p \in A$ que divide a los coeficientes $a_1, \ldots, a_d$ pero $p^2 \nmid a_d$. Entonces el polinomio f es irreducible.*

Demostración. Con las notaciones del Lema III.1, $\widehat{f}(\mathtt{t}) := \sum_{k=0}^{d} a_k \mathtt{t}^{n-k}$ es primitivo, pues sus coeficientes son, en distinto orden, los de f y, por el Criterio de Eisenstein, es irreducible en $A[\mathtt{t}]$. Esto implica, por el Lema III.1, que f es irreducible en $A[\mathtt{t}]$. □

El siguiente resultado, también original, proporciona información sobre los grados de los factores irreducibles de un polinomio con coeficientes en un DFU si estos cumplen ciertas condiciones "tipo Criterio de Eisenstein".

Lema III.9 *Sean A un* DFU *y $f(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i$ un polinomio primitivo de grado d. Supongamos que existen un elemento irreducible $p \in A$ y dos enteros $k \in \{0, \ldots, d-1\}$ y $n \geq 1$ tales que p divide a $a_0, \ldots, a_k$ y p^n divide a a_0 pero p^{n+1} no divide a a_0. Entonces f tiene algún factor irreducible de grado mayor que $\frac{k}{n}$.*

Demostración. Como $A[\mathtt{t}]$ es un DFU y f es primitivo, podemos escribir $f := f_1 \cdots f_m$ como producto de polinomio irreducibles en $A[\mathtt{t}]$, todos ellos de grado mayor o igual que 1. reordenando los factores si es preciso podemos suponer que $\deg(f_i) \leq \deg(f_m)$ para $i = 1, \ldots, m$. Se tiene $a_0 = f(0) = f_1(0) \cdots f_m(0)$, y distinguimos dos casos.

Caso 1. Supongamos que $p | f_j(0)$ para todo $j = 1, \ldots, m$. Entonces $p^n | a_0$ y, como $p^{n+1} \nmid a_0$, deducimos que $m \leq n$. Por otro lado,

$$d = \deg(f) = \deg\left(\prod_{i=1}^{m} f_i\right) = \sum_{i=1}^{m} \deg(f_i) \leq m \cdot \max\{\deg(f_i) : i = 1, \ldots, d\} = m \deg(f_m),$$

por lo que $k/n < d/n \leq d/m \leq \deg(f_m)$, y la prueba en este caso está acabada.

Caso 2. Supongamos que existe algún índice $j \in \{1, \ldots, m\}$ tal que $p \nmid f_j(0)$. Reordenando los factores $f_1, \ldots, f_m$ si es preciso podemos suponer que $p|f_j(0)$ para $j = 1, \ldots, r$ y $p \nmid f_j(0)$ para $j = r+1, \ldots, m$, donde $r < m$. Definimos entonces

$$g(\mathtt{t}) := \prod_{j=1}^{r} f_j(\mathtt{t}) = \sum_{i=1}^{\deg(g)} b_i \mathtt{t}^i \in A[\mathtt{t}] \quad \text{y} \quad h(\mathtt{t}) := \prod_{j=r+1}^{m} f_j(\mathtt{t}) = \sum_{i=1}^{\deg(h)} c_i \mathtt{t}^i \in A[\mathtt{t}],$$

que cumplen la igualdad $f = gh$. Esto implica, en particular, que g es primitivo, por serlo f. Nótese que $p \nmid c_0$ y $p^r | g(0)|f(0) = a_0$. Como $p^{n+1} \nmid a_0$ se tiene $r < n+1$, esto es, $r \leq n$. Además $p|g(0) = b_0$ y, como g es primitivo, el conjunto $I := \{i = 1, \ldots, \deg(g) : p \nmid b_i\}$ no es vacío y definimos $s := \min(I) \leq \deg(g)$. Escribimos

$$a_s = b_0 c_s + b_1 c_{s-1} + \cdots + b_{s-1} c_1 + b_s c_0.$$

Como p divide a los s primeros sumandos del miembro de la derecha pero no divide a $b_s c_0$ pues no divide ni a b_s ni a c_0, se tiene $p \nmid a_s$, luego $k < s$. Por ello,

$$r \cdot \left(\frac{k}{n}\right) \leq n \cdot \left(\frac{k}{n}\right) = k < s \leq \deg(g) \leq r \cdot \max\{\deg(f_j) : j = 1, \ldots, r\},$$

y por tanto,

$$\frac{k}{n} < \max\{\deg(f_j) : j = 1, \ldots, r\} \leq \max\{\deg(f_j) : j = 1, \ldots, m\}.$$

□

Observación III.10 El Lema III.9 con $n = 1$ y $k = d - 1$ es el Criterio de Eisenstein III.3.

Tanto el enunciado como la prueba del Criterio de Netto que presentamos a continuación son semejantes a los del Criterio de Eisenstein; ambos se apoyan en la divisibilidad o no de los coeficientes del polinomio por un primo y sus potencias.

Proposición III.11 (Criterio de Netto) *Sean A un* DFU *y $f(\mathtt{t}) := \sum_{k=0}^{d} a_k \mathtt{t}^k$ un polinomio primitivo de grado impar $d = 2m+1$. Supongamos que existe un elemento irreducible $p \in A$ tal que $p|a_k$ para $m < k \leq 2m$, $p^2|a_k$ para $0 \leq k \leq m$ y $p^3 \nmid a_0$. Entonces f es irreducible en $A[\mathtt{t}]$.*

Demostración. Obsérvese que $p \nmid a_{2m+1}$ por ser f primitivo. Si el polinomio f fuese reducible en $A[\mathtt{t}]$ existirían polinomios $g, h \in A[\mathtt{t}] \setminus A$ de grados r y s respectivamente tales que $f = gh$. Como $r + s = d$ es impar podemos suponer sin pérdida de generalidad que $s = \deg(h) < \deg(g) = r$, luego

$$2s = 2\deg(h) < \deg(g) + \deg(h) = \deg(gh) = \deg(f) = 2m + 1,$$

por lo que $1 \leq s \leq m$. Escribimos

$$g(\mathtt{t}) := \sum_{i=0}^{r} b_i \mathtt{t}^i \quad \text{y} \quad h(\mathtt{t}) := \sum_{j=0}^{s} c_j \mathtt{t}^j,$$

donde cada $b_i, c_j \in A$. Como $p \nmid a_{2m+1} = b_r c_s$ se deduce que $p \nmid b_r$ y $p \nmid c_s$. Por tanto,

$$I := \{0 \leq i \leq r : p \nmid b_i\} \quad \text{y} \quad J := \{0 \leq j \leq s : p \nmid c_j\}$$

son conjuntos no vacíos, ya que $r \in I$ y $s \in J$, luego existen $k := \text{mín}(I)$ y $\ell := \text{mín}(J)$. Nótese que

$$a_{k+\ell} = \sum_{i+j=k+\ell} b_i c_j = b_k c_\ell + \sum_{i+j=k+\ell,\, i \neq k} b_i c_j$$

donde $b_i = 0$ si $i > r$ y $c_j = 0$ si $j > s$. Para cada pareja de índices $(i,j) \neq (k,\ell)$ con $i + j = k + \ell$, se cumple que $i < k$ o $j < \ell$. En consecuencia, $p | b_i$ o $p | c_j$, lo que implica que $p | b_i c_j$. Por tanto p divide a la suma $\sum_{i+j=k+\ell, i\neq k} b_i c_j$, pero no a $b_k c_\ell$, por lo que $p \nmid a_{k+\ell}$. Las condiciones impuestas a p implican que $k + \ell = 2m + 1 = r + s$ y, como $k \leq r$ y $\ell \leq s$, resulta $k = r$ y $\ell = s$. Por tanto, $p | b_i$ y $p | c_j$ para $0 \leq i \leq r-1$ y $0 \leq j \leq s-1$. Calculamos

$$a_s = \sum_{i=0}^{s} b_i c_{s-i} = b_0 c_s + \sum_{i=1}^{s} b_i c_{s-i}.$$

Nótese que $p^2 | a_s$ pues $s \leq m$, pero $p | b_i$ para $0 \leq i \leq s \leq r-1$ y $p | c_{s-i}$ para $1 \leq i \leq s$. Por tanto p^2 divide a a_s y a cada sumando $b_i c_{s-i}$ con $1 \leq i \leq s$, así que $p^2 | b_0 c_s$. Como A es un DFU y p no divide a c_s deducimos que $p^2 | b_0$, lo que junto al hecho de que $p | c_0$ implica que $p^3 | b_0 c_0 = a_0$, contra la hipótesis. □

Ejemplo III.12 Se deduce directamente del Criterio de Netto que si A es un DFU, d es un entero positivo impar y $p \in A$ es un elemento irreducible, entonces el polinomio $\mathtt{t}^d - p^2$ es irreducible en $A[\mathtt{t}]$.

Comentario III.13 La condición sobre la imparidad del grado del polinomio es fundamental para la validez del Criterio de Netto. En efecto, tomando en el ejemplo anterior $d = 2k$, con $k \in \mathbb{N}$, se tiene $\mathtt{t}^{2k} - p^2 = \left(\mathtt{t}^k - p\right)\left(\mathtt{t}^k + p\right)$, luego el polinomio $\mathtt{t}^{2k} - p^2$ es reducible.

CAPÍTULO IV

Irreducibilidad en $\mathbb{Z}[\mathtt{t}]$. Criterio de Cohn

Esta sección estudiamos Criterios de irreduciblidad de polinomios en $\mathbb{Z}[\mathtt{t}]$. Comenzamos presentando un ejemplo del modo de argumentar en este contexto. Después probamos el *Criterio de Cohn,* que pone de manifiesto la relación entre polinomios irreducibles en $\mathbb{Z}[\mathtt{t}]$ y números primos. Además, veremos cómo este criterio esconde una conjetura muy profunda, denominada *Conjetura de Bunyakovsky,* que enunciaremos al final de la sección, y sobre la que se puede consultar en [OR]. Abreviaremos $\mathtt{c}(f) = \mathtt{c}_{\mathbb{Z}}(f)$ para cada polinomio $f \in \mathbb{Z}[\mathtt{t}]$.

Ejemplo IV.1 Sean $d \geq 2$ un entero y $1 < a_1 < \cdots < a_{d-1} < a_d = p$ números enteros, donde p es primo. Entonces el polinomio $f(\mathtt{t}) := \mathtt{t}^d + \sum_{i=1}^{d} a_i \mathtt{t}^{d-i}$ es irreducible en $\mathbb{Z}[\mathtt{t}]$.

(2) Dados números primos $p_1 < p_2 < \cdots < p_d$ primos el polinomio $f(\mathtt{t}) := \mathtt{t}^d + \sum_{i=1}^{d} p_i \mathtt{t}^{d-i}$ es irreducible en $\mathbb{Z}[\mathtt{t}]$.

Es obvio que el apartado (2) es un caso particular del primero, por lo que sólo necesitamos demostrar (1). Como f es mónico, si fuese reducible en $\mathbb{Z}[\mathtt{t}]$ existirían polinomios mónicos $g, h \in \mathbb{Z}[\mathtt{t}]$ tales que $f = gh$ y $\deg(g), \deg(h) \geq 1$. Sean

$$g(\mathtt{t}) := \mathtt{t}^r + \sum_{j=1}^{r} b_j \mathtt{t}^{r-j} \quad \text{y} \quad h(\mathtt{t}) := \mathtt{t}^s + \sum_{k=1}^{s} c_k \mathtt{t}^{s-k}.$$

Como $p = f(0) = g(0)h(0) = b_r c_s$ y p es primo podemos suponer que $b_r = p$ y $c_s = 1$. Sean $\alpha_1, \ldots, \alpha_s \in \mathbb{C}$, no necesariamente distintos, tales que

$$h(\mathtt{t}) := \prod_{k=1}^{s} (\mathtt{t} - \alpha_k) \quad \rightsquigarrow \quad \pm 1 = c_s = h(0) = (-1)^s \prod_{k=1}^{s} \alpha_k.$$

Para llegar a contradicción basta ver que el módulo de cada raíz de f es mayor que 1. En tal caso, como las raíces de h lo son de f, cada $|\alpha_k| > 1$ para $1 \leq k \leq s$, así que

$$1 = \left| (-1)^s \prod_{k=1}^{s} \alpha_k \right| = \prod_{k=1}^{s} |\alpha_k| > 1,$$

lo que es imposible. Sea pues $\alpha \in \mathbb{C}$ una raíz de f y supongamos, por reducción al absurdo, que $|\alpha| \leq 1$. Consideramos el producto

$$\varphi(\mathtt{t}) := (\mathtt{t} - 1) f(\mathtt{t}) = \sum_{i=0}^{d} \gamma_i \mathtt{t}^{d+1-i} - p \in \mathbb{Z}[\mathtt{t}].$$

Como $\varphi(1) = 0$, se tiene $\sum_{i=0}^{d} \gamma_i = p$. Además $\varphi(\alpha) = 0$, luego $\sum_{i=0}^{d} \gamma_i \alpha^{d+1-i} = p$, y así

$$\gamma_i = a_i - a_{i-1} > 0 \ \text{ para cada } \ i \geq 2, \ \ \gamma_1 = a_1 - 1 > 0 \ \text{ y } \ \gamma_0 = 1.$$

De este modo, como cada $\gamma_i > 0$ y $|\alpha| \leq 1$, se deduce de la desigualdad triangular que

$$p = \Big| \sum_{i=0}^{d} \gamma_i \alpha^{d+1-i} \Big| \leq \sum_{i=0}^{d} \gamma_i \cdot |\alpha|^{d+1-i} \leq \sum_{i=0}^{d} \gamma_i = p. \tag{IV.1}$$

Esto implica que $\big| \sum_{i=0}^{d} \gamma_i \alpha^{d+1-i} \big| = \sum_{i=0}^{d} \gamma_i \cdot |\alpha|^{d+1-i}$, es decir, la desigualdad triangular es en este caso una igualdad, por lo que existen números reales $\{c_i : 1 \leq i \leq d\}$ tales que cada $c_i \geq 0$ y $\gamma_d \alpha = c_i \gamma_{d-i} \alpha^{1+i}$.

Si $c := c_1$ se tiene $\gamma_d \alpha = c \gamma_{d-1} \alpha^2$ y, como $\alpha \neq 0$, se tiene $c \neq 0$ y $\alpha = \gamma_d / c\gamma_{d-1}$ es un número real positivo. Así, como también la segunda desigualdad de (IV.1) es una igualdad,

$$\sum_{i=0}^{d} \gamma_i \alpha^{d+1-i} = \sum_{i=0}^{d} \gamma_i \quad \text{y} \quad 0 < \alpha \leq 1,$$

por lo que $\alpha = 1$, y esto no es posible ya que $f(1) = 1 + \sum_{i=1}^{d} a_i > 0$.

Antes de enunciar el resultado fundamental de esta sección, veamos una proposición previa que ilustra la relación entre polinomios irreducibles y números primos.

Proposición IV.2 *Sea $f(\mathtt{t}) := a_0 + a_1\mathtt{t} + \cdots + a_d\mathtt{t}^d \in \mathbb{Z}[\mathtt{t}]$ un polinomio no nulo. Supongamos que existen $m_1, \ldots, m_{2d+1} \in \mathbb{Z}$ distintos dos a dos tales que $f(m_i) = \pm p_i$ con p_i primo o 1 para todo $i = 1, \ldots, 2d+1$. Entonces f es irreducible en $\mathbb{Z}[\mathtt{t}]$.*

Demostración. Veamos primero que f es primitivo. En caso contrario su contenido es, necesariamente, un número primo p, y existe un polinomio primitivo $f_1 \in \mathbb{Z}[\mathtt{t}]$ tal que $f = pf_1$. Entonces $f_1(m_i) = \pm 1$ para $i = 1, \ldots, 2d+1$, es decir, el polinomio $f_1^2 - 1$, que tiene grado $2d$, tiene a los $2d+1$ enteros $m_1, \ldots, m_{2d+1}$ por raíces, lo que es absurdo.

Por tanto, si f fuese reducible en $\mathbb{Z}[\mathtt{t}]$ existirían $g, h \in \mathbb{Z}[\mathtt{t}]$ de grado mayor o igual que 1 tales que $f = gh$. Denotemos

$$I = \{i = 1, \ldots, 2d+1 : \, g^2(m_i) = 1\} \quad \text{y} \quad J = \{i = 1, \ldots, 2d+1 : \, h^2(m_i) = 1\}.$$

Como $g(m_i)h(m_i) = f(m_i) = \pm p_i$ donde p_i es primo o 1 se tiene

$$\{1, \ldots, 2d+1\} = I \cup J. \tag{IV.2}$$

Cada m_i con $i \in I$ es raíz del polinomio $g^2 - 1$, que no es nulo, luego

$$\mathrm{Card}(I) \leq \deg(g^2 - 1) = 2\deg(g).$$

Por la misma razón, $\mathrm{Card}(J) \leq \deg(h^2 - 1) = 2\deg(h)$, y sustituyendo estos valores en (IV.2) llegamos a una contradicción:

$$\begin{aligned} 2d+1 = \mathrm{Card}(I \cup J) &\leq \mathrm{Card}(I) + \mathrm{Card}(J) \leq 2\deg(g) + 2\deg(h) \\ &= 2(\deg(g) + \deg(h)) = 2\deg(f) = 2d, \end{aligned}$$

por lo que f es irreducible en $\mathbb{Z}[\mathtt{t}]$. □

Ejemplo IV.3 Sea $f(\mathtt{t}) := \mathtt{t}^4 - 2\mathtt{t} + 8$ que tiene grado $d = 4$. Observamos que

$$f(1) = 7,\ \ f(-1) = 11,\ \ f(3) = 83,\ \ f(-5) = 643,\ \ f(-7) = 2423,\ \ f(9) = 6551$$
$$f(11) = 14627,\ \ f(-17) = 83563 \quad \text{y} \quad f(-19) = 130367.$$

Hemos encontrado $2 \cdot 4 + 1 = 9$ enteros distintos en los que f toma valores primos y se deduce de la proposición anterior que f es irreducible en $\mathbb{Z}[\mathtt{t}]$.

Observación IV.4 Sea $g(\mathtt{t}) := b_0 + b_1\mathtt{t} + \cdots + b_d\mathtt{t}^d \in \mathbb{Z}[\mathtt{t}]$ y supongamos que existen $m, n \in \mathbb{Z}$ tales que $g(m) = 1$ y $g(n) = -1$. Entonces, $|m - n| \leq 2$. En efecto,

$$1 = g(m) = \sum_{k=0}^{d} b_k m^k \ \text{ y } \ -1 = g(n) = \sum_{k=0}^{d} b_k n^k \ \rightsquigarrow \ 2 = g(m) - g(n) = \sum_{k=1}^{d} b_k(m^k - n^k). \tag{IV.3}$$

Veamos que cada $m^k - n^k$ es múltiplo de $m - n$.

El polinomio $g_k(\mathtt{t}) := \mathtt{t}^k - n^k \in \mathbb{Z}[\mathtt{t}]$ cumple $g_k(n) = 0$ luego, por la Regla de Ruffini, existe $h_k \in \mathbb{Z}[\mathtt{t}]$ tal que $g_k(\mathtt{t}) = (\mathtt{t} - n)h_k(\mathtt{t})$. Evaluamos ambos miembros en $\mathtt{t} = m$:

$$m^k - n^k = g_k(m) = (m - n)h_k(m) \in (m - n)\mathbb{Z},$$

lo que sustituido en (IV.3) implica que $m - n$ divide a 2, por lo que $|m - n| \leq 2$.

La observación anterior sugiere el siguiente corolario que está íntimamente relacionado con la Proposición IV.2.

Corolario IV.5 *Sea $f(\mathtt{t}) = a_0 + a_1\mathtt{t} + \cdots + a_d\mathtt{t}^d \in \mathbb{Z}[\mathtt{t}]$ un polinomio no nulo. Supongamos que existen $m_1, \ldots, m_{d+1} \in \mathbb{Z}$ tales que $|m_i - m_j| > 2$ si $i \neq j$ y $f(m_i) = \pm p_i$ con p_i primo o 1 para todo $i = 1, \ldots, d + 1$. Entonces f es irreducible en $\mathbb{Z}[\mathtt{t}]$.*

Demostración. Veamos que f es primitivo. En caso contrario su contenido es, necesariamente, un número primo p, y existe un polinomio primitivo $f_1 \in \mathbb{Z}[\mathtt{t}]$ tal que $f = pf_1$. Entonces $|f(m_i)| = 1$ para $i = 1, \ldots, d + 1$. Además, por la Observación anterior IV.4, existe $\varepsilon \in \{-1, +1\}$ tal que $f(m_i) = \varepsilon$ para $i = 1, \ldots, d + 1$. Esto es imposible porque implica que el polinomio $f_i - \varepsilon$ cuyo grado es d, tiene al menos $d + 1$ raíces.

Por tanto, si f fuese reducible en $\mathbb{Z}[\mathtt{t}]$ existirían $g, h \in \mathbb{Z}[\mathtt{t}]$ de grado mayor o igual que 1 tales que $f = gh$. Como $g(m_1)h(m_1) = \pm p_1$ donde p_i es primo o 1, alguno de los números $g(m_1)$ y/o $h(m_1)$ vale 1 o -1 y, sin pérdida de generalidad, podemos suponer que $g(m_1) = \varepsilon_1 \in \{-1, +1\}$. Esto implica, por la Observación IV.4, que $g(m_j) \neq -\varepsilon_1$ para $j = 2, \ldots, d + 1$.

Obsérvese que $\deg(g) = \deg(f) - \deg(h) \leq d - 1$ luego el valor que toma g en al menos dos elementos del conjunto $\{m_1, \ldots, m_{d+1}\}$ es distinto de ε_1, ya que en caso contrario el polinomio $g - \varepsilon_1$, que no es nulo, tendría más raíces que grado. Tras reordenar si es preciso podemos suponer que $g(m_d) \neq \varepsilon_1$ y $g(m_{d+1}) \neq \varepsilon_1$. Como $\pm p_j = g(m_j)h(m_j)$ concluimos, empleando de nuevo la Observación IV.4, que existe $\varepsilon_2 \in \{-1, +1\}$ tal que $h(m_d) = h(m_{d+1}) = \varepsilon_2 \in \{-1, +1\}$. Para terminar denotemos

$$I_1 = \{i = 1, \ldots, d + 1 :\ g(m_i) = \varepsilon_1\} \quad \text{e} \quad I_2 = \{i = 1, \ldots, d + 1 :\ h(m_i) = \varepsilon_2\}.$$

Se tiene $\mathrm{Card}(I_1) \leq \deg(g - \varepsilon_1) = \deg(g)$ y $\mathrm{Card}(I_2) \leq \deg(h - \varepsilon_2)\deg(h)$. Como

$$\{1, \ldots, d+1\} = I_1 \cup I_2, \tag{IV.4}$$

$$d + 1 = \mathrm{Card}(I_1 \cup I_2) \leq \mathrm{Card}(I) + \mathrm{Card}(I_2) \leq \deg(g) + \deg(h) = \deg(f) = d,$$

que es una contradicción, por lo que f es irreducible en $\mathbb{Z}[\mathtt{t}]$. □

Ejemplo IV.6 Se deduce del Corolario IV.5 que el polinomio

$$f(\mathtt{t}) = \mathtt{t}^6 - 3\mathtt{t}^5 - 87\mathtt{t}^4 + 118\mathtt{t}^3 - 33\mathtt{t}^2 + 21\mathtt{t} - 1$$

es irreducible en $\mathbb{Z}[\mathtt{t}]$ pues toma los siguientes valores:

$$f(-22) = 107187629,\ \ f(-8) = -58601,\ \ f(-4) = -23269,\ \ f(0) = -1,$$
$$f(12) = 634859,\ \ f(18) = 19888469 \text{ y } f(30) = 588786929$$

y, salvo $f(0) = -1$, los restantes son primos u opuestos de primos.

Ejemplo IV.7 Vamos a demostrar que el polinomio $f(\mathtt{t}) := \mathtt{t}^4 + 2\mathtt{t}^3 - 13\mathtt{t}^2 + 10\mathtt{t} + 3$ es irreducible en $\mathbb{Z}[\mathtt{t}]$. Como es primitivo es suficiente probar, en virtud del Corolario I.15, que lo es en $\mathbb{Q}[\mathtt{t}]$. Como vimos en el Criterio de la homotecia, Proposición I.8, esto último equivale a que sea irreducible en $\mathbb{Q}[\mathtt{t}]$ el polinomio

$$f_3(\mathtt{t}) = f(3\mathtt{t}) := 3g(\mathtt{t}), \quad \text{donde} \quad g(\mathtt{t}) := 27\mathtt{t}^4 + 18\mathtt{t}^3 - 39\mathtt{t}^2 + 10\mathtt{t} + 1.$$

Como 3 es una unidad en $\mathbb{Q}$ basta demostrar que g es irreducible en $\mathbb{Q}[\mathtt{t}]$. Para ello aplicamos el Corolario IV.5, pues se cumple:

$$f(0) = 1,\ \ f(1) = 171,\ \ f(4) = 74811,\quad f(6) = 375371,\quad f(10) = 2842011,$$
$$f(15) = 14190011,\ \ f(22) = 64979211,\ \ f(36) = 461392571 \text{ y } \quad f(45) = 112278601,$$

y, salvo $f(0) = 1$, los restantes valores son primos.

El Corolario IV.5 puede refinarse si los coeficientes del polinomio involucrado cumplen ciertas condiciones. Esto constituye un criterio útil para decidir la irreducibilidad de ciertos polinomios: el Criterio de Cohn, que Polya y Szego atribuyen en [PS] a Arthur Cohn, un estudiante de Schur que vivió en la primera mitad del s. XX.

Teorema IV.8 (Criterio de Cohn) *Sea $p := \sum_{i=0}^{d} a_i 10^i$ la escritura de un entero primo p en base 10. Entonces el polinomio $f(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i$ es irreducible en $\mathbb{Z}[\mathtt{t}]$.*

Este criterio fue generalizado en [BFO] sustituyendo la base 10 por cualquier base mayor o igual que 2. Es decir, se tiene el siguiente criterio de irreducibilidad.

Teorema IV.9 (Criterio de Cohn generalizado) *Sea $p := \sum_{i=0}^{d} a_i b^i$ la escritura de un entero primo p en base $b \geq 2$. Entonces $f(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i$ es irreducible en $\mathbb{Z}[\mathtt{t}]$.*

Podemos reformular este criterio de modo más intuitivo, pues el criterio de Cohn generalizado es equivalente a la siguiente afirmación:

"*Sea* $f(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i \in \mathbb{Z}[\mathtt{t}]$ *de grado* d *tal que* $0 \leq a_i < b$ *para cierto entero positivo* b*, y supongamos que* $f(b)$ *es un número primo. Entonces* f *es irreducible en* $\mathbb{Z}[\mathtt{t}]$".

Antes de demostrar el Teorema IV.9 necesitamos varios lemas auxiliares.

Lema IV.10 *Sean* $f(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i \in \mathbb{C}[\mathtt{t}]$ *un polinomio de grado* d *con coeficientes en* $\mathbb{C}$ *y* $\alpha \in \mathbb{C}$ *una raíz de* f*. Sea* $H := \max\left\{\left|\frac{a_i}{a_d}\right| : 0 \leq i \leq d-1\right\}$*. Entonces,* $|\alpha| < H + 1$.

Demostración. Si $H = 0$ entonces $f(\mathtt{t}) = \mathtt{t}^d$ así que $\alpha = 0$ y $|\alpha| = 0 < H + 1$. Suponemos pues que $H > 0$. Si $|\alpha| \leq 1$ entonces $|\alpha| < H + 1$ y nada hay que probar. Supongamos que $|\alpha| > 1$. Como α es una raíz de f, tenemos:

$$0 = f(\alpha) = a_d\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 \quad \rightsquigarrow \quad -a_d\alpha^d = a_{d-1}\alpha^{d-1} + \cdots + a_0,$$

y dividiendo por $|a_d|$ ambos miembros y aplicando la desigualdad triangular:

$$|\alpha^d| \leq \left|\frac{a_{d-1}}{a_d}\cdot\right| \left|\alpha^{d-1}\right| + \cdots + \left|\frac{a_0}{a_d}\right| \leq H\big(1 + |\alpha| + \cdots + |\alpha|^{d-1}\big) = H \cdot \left(\frac{|\alpha^d| - 1}{|\alpha| - 1}\right). \quad \text{(IV.5)}$$

Como $|\alpha| - 1 > 0$, multiplicando por este factor los dos miembros de la desigualdad (IV.5) se tiene:

$$|\alpha^{d+1}| - |\alpha^d| \leq H\big(|\alpha|^d - 1\big) < H|\alpha|^d,$$

y dividiendo ambos miembros por $|\alpha|^d$ obtenemos $|\alpha| - 1 < H$, como queríamos. □

Lema IV.11 *Sean* $f(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i \in \mathbb{Z}[\mathtt{t}]$ *primitivo de grado* d *y*

$$H := \max\left\{\left|\frac{a_i}{a_d}\right| : 0 \leq i \leq d-1\right\}.$$

Si existe un entero $n \geq H + 2$ *tal que* $f(n)$ *es primo, entonces* f *es irreducible en* $\mathbb{Z}[\mathtt{t}]$.

Demostración. Si f fuese reducible en $\mathbb{Z}[\mathtt{t}]$, y puesto que es primitivo, existen $g, h \in \mathbb{Z}[\mathtt{t}]$ de grado positivo tales que $f(\mathtt{t}) = g(\mathtt{t})h(\mathtt{t})$. Evaluando esta igualdad en $\mathtt{t} = n$, y ya que $p := f(n) = g(n)h(n)$ es primo, podemos suponer que $g(n) = 1$. Sean $\alpha_1, \ldots, \alpha_{\deg(g)}$ las raíces, no necesariamente distintas, de g en $\mathbb{C}$. Por el Lema IV.10 cada $|\alpha_i| < n$, luego

$$g(\mathtt{t}) = \ell(g) \prod_{i=1}^{\deg(g)} (\mathtt{t} - \alpha_i) \quad \rightsquigarrow \quad 1 = |g(n)| = \ell(g) \cdot \prod_{i=1}^{\deg(g)} |n - \alpha_i| \geq \ell(g) \prod_{i=1}^{\deg(g)} (n - |\alpha_i|).$$

Utilizando de nuevo el Lema IV.10, $n - |\alpha_i| > n - (H + 1)$ para cada índice i, y se tiene

$$1 = |g(n)| > \ell(g) \prod_{i=1}^{\deg(g)} (n - (H + 1)) \geq 1,$$

que es una contradicción, lo que demuestra que f es irreducible en $\mathbb{Z}[\mathtt{t}]$. □

Ejemplo IV.12 Se deduce del Lema IV.11 que $f(\mathtt{t}) := 3\mathtt{t}^5 + 2\mathtt{t}^2 + \mathtt{t} + 3$ es irreducible en $\mathbb{Z}[\mathtt{t}]$ pues en este caso $H = 1$ y $f(5) = 9433$ es primo.

Lema IV.13 *Sea $f(\mathtt{t}) := a_d\mathtt{t}^d + a_{d-1}\mathtt{t}^{d-1} + \cdots + a_1\mathtt{t} + a_0 \in \mathbb{Z}[\mathtt{t}]$ un polinomio de grado $d \geq 2$. Supongamos que $a_d \geq 1$, que $a_{d-1} \geq 0$, y sea ρ un número real positivo tal que que $|a_i| \leq \rho$ para todo $i = 1, ..., d-2$. Sea $\alpha \in \mathbb{C}$ una raíz de f. Entonces se cumple una de las dos condiciones siguientes:*

(i) *La parte real* $\Re(\alpha) \leq 0$ *o* (ii) $|\alpha| < \frac{1+\sqrt{1+4\rho}}{2}$.

Demostración. Sea $z \in \mathbb{C}$ tal que $|z| > 1$ y $\Re(z) > 0$. Entonces

$$\left|\frac{f(z)}{z^d}\right| = \left|a_d + \frac{a_{d-1}}{z} + \cdots + \frac{a_1}{z^{d-1}} + \frac{a_0}{z^d}\right|, \quad \text{y por tanto}$$

$$\left|\frac{f(z)}{z^d}\right| \geq \left|a_d + \frac{a_{d-1}}{z}\right| - \left|\frac{a_{d-2}}{z^2} + \cdots + \frac{a_1}{z^{d-1}} + \frac{a_0}{z^d}\right|. \tag{IV.6}$$

Como cada $|a_i| \leq \rho$ para $i = 0, \ldots, d-2$ se deduce de la desigualdad (IV.6)

$$\begin{aligned}
\left|\frac{f(z)}{z^d}\right| &\geq \left|a_d + \frac{a_{d-1}}{z}\right| - \rho\left(\frac{1}{|z|^2} + \cdots + \frac{1}{|z|^d}\right) = \left|a_d + \frac{a_{d-1}}{z}\right| - \frac{\rho}{|z|^2}\left(1 + \frac{1}{|z|} + \cdots + \frac{1}{|z|^{d-2}}\right) \\
&= \left|a_d + \frac{a_{d-1}}{z}\right| - \frac{\rho}{|z|^2}\left(\frac{1 - \frac{1}{|z|^{d-1}}}{1 - \frac{1}{|z|}}\right) = \left|a_d + \frac{a_{d-1}}{z}\right| - \frac{\rho}{|z|^2}\left(\frac{|z|^{d-1} - 1}{|z|^{d-2}\big(|z| - 1\big)}\right) \\
&= \left|a_d + \frac{a_{d-1}}{z}\right| - \frac{\rho\left(|z|^{d-1} - 1\right)}{|z|^d\big(|z| - 1\big)} = \left|a_d + \frac{a_{d-1}}{z}\right| - \rho\left(\frac{1}{|z|\big(|z| - 1\big)} - \frac{1}{|z|^d(|z| - 1)}\right) \\
&> \left|a_d + \frac{a_{d-1}}{z}\right| - \frac{\rho}{|z|\big(|z| - 1\big)} \geq \Re\left(a_d + \frac{a_{d-1}}{z}\right) - \frac{\rho}{|z|\big(|z| - 1\big)} = \Re\left(a_d + \frac{a_{d-1}\overline{z}}{z\overline{z}}\right) \\
&- \frac{\rho}{|z|\big(|z| - 1\big)} = a_d + \frac{a_{d-1}\Re(z)}{z\overline{z}} - \frac{\rho}{|z|\big(|z| - 1\big)} \geq a_d - \frac{\rho}{|z|\big(|z| - 1\big)} \geq 1 - \frac{\rho}{|z|\big(|z| - 1\big)}.
\end{aligned} \tag{IV.7}$$

Por tanto, hemos comprobado que para cada $z \in \mathbb{C}$ tal que $|z| > 1$ y $\Re(z) > 0$ se tiene

$$\left|\frac{f(z)}{z^d}\right| > 1 - \frac{\rho}{|z|\big(|z| - 1\big)} = \frac{|z|^2 - |z| - \rho}{|z|^2 - |z|} = \frac{\big(|z| - \frac{1}{2}\big)^2 - \big(\rho + \frac{1}{4}\big)}{|z|^2 - |z|}. \tag{IV.8}$$

Ya estamos en condiciones de demostrar el enunciado. Sea $\alpha \in \mathbb{C}$ una raíz de f. Podemos suponer que $|\alpha| > 1$ y que $\Re(\alpha) > 0$, pues en caso contrario el resultado es trivialmente cierto. Entonces, por (IV.8),

$$0 = \left|\frac{f(\alpha)}{\alpha^d}\right| > \frac{\big(|\alpha| - \frac{1}{2}\big)^2 - \big(\rho + \frac{1}{4}\big)}{|\alpha|^2 - |\alpha|}.$$

El denominador $|\alpha|^2 - |\alpha| = |\alpha|(|\alpha| - 1)$ de la última fracción es positivo porque $|\alpha| > 1$, luego el numerador es negativo, es decir, $\frac{(2|\alpha|-1)^2}{4} < \frac{1+4\rho}{4}$, esto es, $|\alpha| < \frac{1+\sqrt{1+4\rho}}{2}$. □

Ya podemos demostrar el criterio de Cohn generalizado para toda base $b \geq 3$, dejando el caso $b = 2$ para más adelante.

Teorema IV.14 *Sean $b \geq 2$ un número entero y p un número primo cuya escritura en base b es:*

$$p = a_d b^d + a_{d-1} b^{d-1} + \cdots + a_0, \ \ \textit{donde} \ d \geq 1.$$

Sea $f(\mathtt{t}) := a_d \mathtt{t}^d + a_{d-1}\mathtt{t}^{d-1} + \cdots + a_0$. Entonces:

(1) *El polinomio $f(\mathtt{t})$ es primitivo en $\mathbb{Z}[\mathtt{t}]$.*

(2) *Si $b > 2$ el polinomio $f(\mathtt{t})$ es irreducible en $\mathbb{Z}[\mathtt{t}]$.*

Demostración. (1) Sean $\mathtt{c}(f)$ el contenido de f y $c_k := \frac{a_k}{\mathtt{c}(f)}$, para $k = 0, \ldots, d$. Entonces,

$$p = \sum_{k=0}^{d} a_k b^k = \mathtt{c}(f) \sum_{k=0}^{d} c_k b^k.$$

Si f no fuese primitivo esta igualdad implica que $\mathtt{c}(f) = p$, por lo que $\sum_{k=0}^{d} c_k b^k = 1$. Como cada $c_k \geq 0$ y $c_d \geq 1$ resulta $1 < c_d b^d \leq \sum_{k=0}^{d} c_k b^k = 1$, que es una contradicción.

(2) Supongamos que f es reducible en $\mathbb{Z}[\mathtt{t}]$. Por (1) existen $g, h \in \mathbb{Z}[\mathtt{t}]$ de grado mayor o igual que 1 tales que $f(\mathtt{t}) = g(\mathtt{t})h(\mathtt{t})$. Entonces $p = f(b) = g(b)h(b)$ y podemos suponer que $g(b) = 1$. Sean $\alpha_1, \ldots, \alpha_{\deg(g)}$ las raíces, no necesariamente distintas, de g en $\mathbb{C}$. Entonces,

$$g(\mathtt{t}) = \ell(g) \prod_{i=1}^{\deg(g)} (\mathtt{t} - \alpha_i). \tag{IV.9}$$

Los coeficientes de f son enteros no negativos y f es de grado d, luego $a_d \geq 1$ y $a_{d-1} \geq 0$. Además, $|a_i| \leq b - 1$ para todo $i = 1, ..., d-2$. Aplicando el Lema IV.13 con $\rho := b - 1$, y puesto que cada α_i es raíz de f, deducimos que

$$\text{bien } \Re(\alpha_i) \leq 0, \ \text{ o bien } \ |\alpha_i| \leq \frac{1 + \sqrt{1 + 4(b-1)}}{2}.$$

En el primer caso,

$$|b - \alpha_i| \geq \Re(b - \alpha_i) = b - \Re(\alpha_i) \geq b > 1, \tag{IV.10}$$

mientras que en el segundo, como $1 \leq (b-1) - 1$ por ser $b \geq 3$, multiplicando ambos miembros por $4(b-1)$ y sumando 1 se tiene

$$1 + 4(b-1) \leq 4(b-1)^2 - 4(b-1) + 1 = (2(b-1) - 1)^2.$$

Extrayendo raíces cuadradas en ambos miembros resulta

$$\sqrt{1 + 4(b-1)} \leq 2(b-1) - 1, \quad \text{es decir,} \quad |\alpha_i| < \frac{1 + \sqrt{1 + 4(b-1)}}{2} \leq b - 1.$$

En particular,

$$|b - \alpha_i| \geq |b| - |\alpha_i| > b - (b-1) = 1. \tag{IV.11}$$

De (IV.10) y (IV.11) se deduce que, en cualquier caso, $|b - \alpha_i| > 1$ para $i = 1, \ldots, \deg(g)$, y evaluando en $\mathtt{t} = b$ la igualdad (IV.9) obtenemos una contradicción, por lo que el polinomio f es irreducible en $\mathbb{Z}[\mathtt{t}]$:

$$1 = |g(b)| = \ell(g) \prod_{i=1}^{\deg(g)} |b - \alpha_i| > 1, \qquad \square$$

Para abordar el caso $b = 2$ necesitamos refinar el Lema IV.13.

Lema IV.15 *Sea $\alpha \in \mathbb{C}$ una raíz del polinomio $f(\mathtt{t}) := a_d\mathtt{t}^d + a_{d-1}\mathtt{t}^{d-1} + \cdots + a_0$ donde cada $a_i \in \{0,1\}$ y $a_d \neq 0$. Denotemos $\Phi := \frac{1+\sqrt{5}}{2}$ la razón áurea.*

(1) *Si $|\arg(\alpha)| < \frac{\pi}{4}$, entonces $|\alpha| < \frac{3}{2}$.*

(2) *Si $|\arg(\alpha)| \geq \frac{\pi}{4}$, entonces $|\Re(\alpha)| < \frac{\Phi}{\sqrt{2}}$.*

(3) *En cualquier caso, $|\Re(\alpha)| < \frac{3}{2}$.*

Demostración. Si $d = 1$, entonces $f(\mathtt{t}) = \mathtt{t}$ o $f(\mathtt{t}) = \mathtt{t}+1$, cuyas raíces son, respectivamente, $\alpha = 0$ y $\alpha = -1$. En el primer caso $\arg(0) = 0 < \frac{\pi}{4}$ y $|\alpha| = 0 < \frac{3}{2}$. En el segundo $\arg(\alpha) = \pi$ y $|\Re(\alpha)| = 1 < \frac{\Phi}{\sqrt{2}}$. Estudiamos ahora el caso $d = 2$. Existen cuatro polinomios de grado 2 cuyos coeficientes son ceros y unos:

$$f_1(\mathtt{t}) := \mathtt{t}^2;\ \ f_2(\mathtt{t}) := \mathtt{t}^2 + \mathtt{t};\ \ f_3(\mathtt{t}) := \mathtt{t}^2 + 1 \ \text{ y } \ f_4(\mathtt{t}) := \mathtt{t}^2 + \mathtt{t} + 1.$$

Las raíces de f_1 y f_2 son 0 y -1 y acabamos de ver que ambos casos satisfacen el enunciado. Las raíces de f_3 son $\pm\mathtt{i}$, donde $\mathtt{i} := \sqrt{-1}$ cuyos argumentos son $\frac{\pi}{2}$ y $\frac{3\pi}{2}$. La parte real de ambas raíces es nula, y se cumple (2). Por último, las raíces de f_4 son $e^{2\pi\mathtt{i}/3}$ y $e^{4\pi\mathtt{i}/3}$ cuyos argumentos son $\pm\frac{2\pi}{3}$, cuyo valor absoluto es mayor que $\frac{\pi}{4}$. El valor absoluto de la parte real de ambas raíces es $\frac{1}{2} < \frac{\Phi}{\sqrt{2}}$.

Suponemos a partir de ahora que $d \geq 3$. Para cada $z \in \mathbb{C} \setminus \{0\}$ tenemos:

$$\left|\frac{f(z)}{z^d}\right| \geq \left|1 + \frac{a_{d-1}}{z} + \frac{a_{d-2}}{z^2}\right| - \left(\frac{1}{|z|^3} + \cdots + \frac{1}{|z|^d}\right), \tag{IV.12}$$

y vamos a demostrar (1). Sea $z \in \mathbb{C}$ tal que $|\arg(z)| < \frac{\pi}{4}$. Entonces $\left|\arg\left(z^2\right)\right| < \frac{2\pi}{4} = \frac{\pi}{2}$. En consecuencia, $\Re(z) > 0$ y $\Re(z^2) > 0$, así que

$$\Re\left(\frac{1}{z}\right) = \Re\left(\frac{\overline{z}}{|z|^2}\right) = \frac{\Re(z)}{|z|^2} > 0 \quad \text{y} \quad \Re\left(\frac{1}{z^2}\right) = \Re\left(\frac{\overline{z}^2}{|z|^4}\right) = \frac{\Re\left(\overline{z}^2\right)}{|z|^4} = \frac{\Re(z^2)}{|z|^4} > 0,$$

luego empleando la desigualdad (IV.12) resulta

$$\begin{aligned}
\left|\frac{f(z)}{z^d}\right| &\geq \left|\Re\left(1 + \frac{a_{d-1}}{z} + \frac{a_{d-2}}{z^2}\right)\right| - \left(\frac{1}{|z|^3} + \cdots + \frac{1}{|z|^d}\right) \\
&= 1 + a_{d-1}\Re\left(\frac{1}{z}\right) + a_{d-2}\Re\left(\frac{1}{z^2}\right) - \left(\frac{1}{|z|^3} + \cdots + \frac{1}{|z|^d}\right) \\
&\geq 1 - \frac{1}{|z|^3}\left(1 + \frac{1}{|z|} + \cdots + \frac{1}{|z|^{d-3}}\right) = 1 - \frac{1}{|z|^3}\left(\frac{1 - \frac{1}{|z|^{d-2}}}{1 - \frac{1}{|z|}}\right) \\
&= 1 - \frac{1}{|z|^2(|z|-1)} + \frac{1}{|z|^d(|z|-1)} > 1 - \frac{1}{|z|^2(|z|-1)} = \frac{|z|^3 - |z|^2 - 1}{(|z|-1)|z|^2}.
\end{aligned} \tag{IV.13}$$

El polinomio $h(\mathtt{t}) := \mathtt{t}^3 - \mathtt{t}^2 - 1$, que evaluado en $\mathtt{t} = |z|$ aparece en el numerador de la última igualdad, sólo tiene una raíz real. En efecto, $h'(\mathtt{t}) = 3\mathtt{t}^2 - 2\mathtt{t} = \mathtt{t}(3\mathtt{t} - 2)$, luego como función real de variable real h sólo es decreciente en el intervalo $\left(0, \frac{2}{3}\right)$. Como $h(0)$ y $h\left(\frac{2}{3}\right)$ son negativos, h tiene una única raíz real que, además, es mayor que $\frac{2}{3}$. De hecho,

$h\left(\frac{3}{2}\right) = \frac{1}{8} > 0$, luego la única raíz real de h está en el intervalo $\left(\frac{2}{3}, \frac{3}{2}\right)$, así que $h(x) > 0$ si $x \geq \frac{3}{2}$. Como para valores de z que cumplen $|\arg(z)| < \frac{\pi}{4}$ se tiene

$$\left|\frac{f(z)}{z^d}\right| > \frac{h(|z|)}{(|z|-1)|z|^2},$$

resulta que si $|\arg(z)| < \frac{\pi}{4}$ y $|z| \geq \frac{3}{2}$, entonces $|f(z)| > 0$ y, en particular, $f(z) \neq 0$. Por tanto, si $\alpha \in \mathbb{C}$ es raíz de f y $|\arg(\alpha)| < \frac{\pi}{4}$, entonces $|\alpha| < \frac{3}{2}$, lo que prueba (1).

Veamos ahora (2). Se deduce del Lema IV.13 aplicado con $\rho := 1$ que $|\alpha| < \frac{1+\sqrt{5}}{2} = \Phi$. Además, $|\cos(\arg(\alpha))| < \cos\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2}$. En consecuencia,

$$|\Re(\alpha)| = |\alpha| \cdot |\cos(\arg(\alpha))| < \frac{\Phi\sqrt{2}}{2} = \frac{\Phi}{\sqrt{2}}.$$

(3) Este apartado se deduce de los dos anteriores porque $|\Re(\alpha)| \leq |\alpha|$ y $\frac{\Phi}{\sqrt{2}} < \frac{3}{2}$. □

Demostramos ya el Teorema de Cohn generalizado para el caso en que la base es $b := 2$.

Teorema IV.16 *Sea p un número primo cuya escritura en base 2 es:*

$$p := a_d 2^d + a_{d-1}2^{d-1} + \cdots + a_0, \quad \textit{donde } d \geq 1.$$

Entonces, el polinomio $f(\mathtt{t}) := a_d\mathtt{t}^d + a_{d-1}\mathtt{t}^{d-1} + \cdots + a_0$ es irreducible en $\mathbb{Z}[\mathtt{t}]$.

Demostración. Vimos en el Teorema IV.14 (1) que f es primitivo, luego si f fuese reducible en $\mathbb{Z}[\mathtt{t}]$ existirían $g, h \in \mathbb{Z}[\mathtt{t}]$ de grado mayor o igual que 1 tales que $f(\mathtt{t}) = g(\mathtt{t})h(\mathtt{t})$, así que $p = f(2) = g(2)h(2)$ y podemos suponer que $g(2) = 1$. Sean $\alpha_1, \ldots, \alpha_{\deg(g)}$ las raíces, no necesariamente distintas, de g en $\mathbb{C}$, y escribimos

$$g(\mathtt{t}) := \ell(g) \prod_{i=1}^{\deg(g)} (\mathtt{t} - \alpha_i). \tag{IV.14}$$

Como cada $a_i \in \{0, 1\}$ estamos en las condiciones del Lema IV.15, luego $|\Re(\alpha_i)| < v := \frac{3}{2}$ para cada $i = 1, \ldots, \deg(g)$. Comprobemos que todos los coeficientes del polinomio

$$\widetilde{g}(\mathtt{t}) := g(\mathtt{t} + v) = \ell(g) \prod_{i=1}^{\deg(g)} (\mathtt{t} + v - \alpha_i) \in \mathbb{R}[\mathtt{t}]$$

son positivos. En efecto, si $\alpha_i \in \mathbb{R}$ entonces $\arg(\alpha_i) = 0 < \frac{\pi}{4}$, y se deduce del Lema IV.15 que $|\alpha| < v$, por lo que los dos coeficientes del polinomio $\mathtt{t} + v - \alpha_i$ son positivos. Si α_i no es real, entonces $\overline{\alpha}_i$ es raíz de f, pues los coeficientes de f son números reales. Por tanto, $\mathtt{t} - \overline{\alpha}_i$ es otro factor de g, y al multiplicar los correspondientes factores de $\widetilde{g}(\mathtt{t})$ resulta

$$(\mathtt{t} + v - \alpha_i)(\mathtt{t} + v - \overline{\alpha}_i) = \mathtt{t}^2 + 2\Re(v - \alpha_i)\mathtt{t} + |v - \alpha_i|^2,$$

cuyos coeficientes son positivos porque $\Re(\alpha_i) < v$. Por ser $\widetilde{g}$ producto de factores con coeficientes reales positivos, sus coeficientes son positivos. Por tanto, los signos de los

coeficientes del polinomio $\widehat{g}(\mathtt{t}) := g(-\mathtt{t}+v)$ son alternos: positivos los de las potencias de exponente par de $\mathtt{t}$ y negativos los de las potencias de exponente impar. Entonces, para todo número real positivo x se cumple $|\widehat{g}(x)| < \widetilde{g}(x)$. Evaluando la desigualdad en $x := \frac{1}{2}$,

$$|g(1)| = \left| g\left(-\frac{1}{2}+\frac{3}{2}\right)\right| = \left|\widehat{g}\left(\frac{1}{2}\right)\right| < \widetilde{g}\left(\frac{1}{2}\right) = g(2) = 1.$$

Pero $g(1) \in \mathbb{Z}$ ya que $g \in \mathbb{Z}[\mathtt{t}]$, luego $|g(1)|$ es un entero no negativo menor que 1. Por ello $g(1) = 0$, así que $f(1) = 0$, y esto es falso ya que

$$f(1) = a_d + a_{d-1} + \cdots + a_0 > 0, \text{ pues cada } a_i = 0, 1 \text{ y } a_d = 1. \qquad \square$$

Ejemplo IV.17 Aplicando el Criterio de Cohn generalizado para $b = 8$ se deduce que el polinomio $f(\mathtt{t}) := 3\mathtt{t}^5 + 2\mathtt{t}^2 + 4\mathtt{t} + 3$ es irreducible en $\mathbb{Z}[\mathtt{t}]$ pues todos sus coeficientes son no negativos y menores que 8 y $f(8) = 98467$ es primo.

Ejemplo IV.18 Se deduce del Teorema IV.16 que los polinomios $f_m(\mathtt{t}) = \mathtt{t}^{2^m} + 1$ son irreducibles en $\mathbb{Z}[\mathtt{t}]$ para $m \in \{0, 1, 2, 3, 4\}$ pues para estos valores de m los números $f_m(2) = 2^{2^m} + 1$ son primos de Fermat.

Comentarios IV.19 (1) Supongamos dado un polinomio primitivo $f \in \mathbb{Z}[\mathtt{t}]$ de grado $d \geq 2$ cuyos coeficientes no nulos son positivos e intentamos demostrar que es irreducible en $\mathbb{Z}[\mathtt{t}]$ aplicando el Teorema de Cohn. Escribimos $f(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i$, y se trata de buscar un entero $b \geq 2$ mayor que cada a_i y tal que $f(b)$ sea primo. En dicha búsqueda nos ayuda observar que, necesariamente, $\operatorname{mcd}(b, a_0) = 1$. En efecto, sea $c := \operatorname{mcd}(b, a_0)$ y escribimos

$$f(b) = a_0 + \sum_{i=1}^{d} a_i b^{i-1} = c \cdot \left(\frac{a_0}{c} + \sum_{i=1}^{d} \frac{a_i b^i}{c}\right). \tag{IV.15}$$

Los dos factores del miembro de la derecha son números enteros positivos y

$$\frac{a_0}{c} + \sum_{i=1}^{d} \frac{a_i b^i}{c} \geq \frac{b^d}{c} \geq \frac{b^2}{c} \geq b \geq 2.$$

De esto y la igualdad (IV.15) se deduce, puesto que $f(b)$ es primo, que $c = 1$.

(2) En la prueba del Criterio de Cohn generalizado la primalidad de $f(b)$ ha jugado un papel relevante, pero no tan imprescindible como en un principio pudiese parecer. El argumento ha consistido en demostrar que f es primitivo, luego en caso de ser reducible es producto de dos polinomios g y h de grados positivos, y deducir que se puede suponer que $g(b) = 1$. Pues bien, veremos a continuación que añadiendo cierta hipótesis adicional podemos sustituir "primo" por "potencia de primo" y seguir concluyendo que $g(b) = 1$, lo que proporciona la contradicción buscada. Esto no es factible sin añadir hipótesis adicionales. Por ejemplo, al escribir $49 = 7^2$ en base 5 se tiene

$$49 = 4 + 4 \cdot 5 + 5^2$$

y el polinomio $f(\mathtt{t}) := 4 + 4\mathtt{t} + \mathtt{t}^2 = (\mathtt{t}+2)^2$ es reducible en $\mathbb{Z}[\mathtt{t}]$. Sin embargo se tiene el siguiente resultado, véase [BBZ].

Teorema IV.20 (Criterio de Cohn para potencias de primo) *Sean $b \geq 2$ y $s \geq 1$ dos enteros y p un número primo. Sea $p^s := \sum_{i=0}^{d} a_i b^i$ la escritura en base b de p^s y consideremos el polinomio $f(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i$. Supongamos que p no divide a $f'(b)$. Entonces f es irreducible en $\mathbb{Z}[\mathtt{t}]$.*

Demostración. Si $s = 1$, el resultado se deduce de los Teoremas IV.14 y IV.16. Supongamos pues que $s \geq 2$ y comprobemos que f es primitivo. En caso contrario tomamos un divisor primo q de su contenido $\mathtt{c}(f)$. Como $q|a_i$ para $i = 0, \ldots, a_d$ resulta que $q|p^s$, luego $q = p$ y esto implica que p divide a $\sum_{i=1}^{d} i a_i b^{i-1} = f'(b)$, lo que es falso.

Así, si f es reducible en $\mathbb{Z}[\mathtt{t}]$ existen $g, h \in \mathbb{Z}[\mathtt{t}]$ de grado mayor o igual que 1 tales que $f = gh$, luego $p^s = f(b) = g(b)h(b)$, así que, sin pérdida de generalidad podemos suponer que $p|h(b)$ y distinguimos dos casos, según que $h(b) \neq \pm p^s$ o $h(b) = \pm p^s$.

Si $h(b) \neq \pm p^s$, entonces $p|g(b)$. En tal caso $f'(b) = g(b)h'(b) + g'(b)h(b) \in p\mathbb{Z}$, contra lo supuesto en el enunciado. Por tanto $h(b) = \pm p^s$, y podemos suponer $g(b) = 1$. A partir de aquí se repite la prueba de IV.14 y IV.16 según que $b \geq 3$ o $b = 2$. □

Observación IV.21 Es natural preguntarse si el siguiente "recíproco"del Criterio de Cohn generalizado es cierto:

Dado un polinomio $f(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i$ irreducible en $\mathbb{Z}[\mathtt{t}]$ de grado d cuyos coeficientes son no negativos, ¿existe $b \in \mathbb{Z}$ tal que $0 \leq a_i < b$ para todo $i = 0, \ldots, b-1$ de modo que $f(b)$ sea primo? Dicho modo, ¿puede ser demostrada aplicando el Criterio de Cohn genaralizado para una base adecuada b la irreducibilidad en $\mathbb{Z}[\mathtt{t}]$ de todo polinomio irreducible cuyos coeficientes son enteros no negativos?

En caso de ser cierto, este resultado proporcionaría un procedimiento para encontrar números primos a partir de polinomios irreducibles. Recordemos que la búsqueda de números primos es fundamental en campos como la criptografía, pues son el fundamento del algoritmo de cifrado RSA, o la informática, pues tradicionalmente se utilizaban números primos como test para procesadores. Pero el enunciado es falso. Basta tomar el polinomio $f(\mathtt{t}) = \mathtt{t}^2 + \mathtt{t} + 2 = \mathtt{t}(\mathtt{t} + 1) + 2$, que es irreducible en $\mathbb{Z}[\mathtt{t}]$, pues es primitivo y carece de raíces enteras, pero cumple que $f(b)$ es un entero par mayor que 2, luego no es primo, para todo entero $b \geq 2$. Este ejemplo se puede plagiar como sigue. Si k es un entero positivo y el polinomio

$$f_k(\mathtt{t}) := \mathtt{t}(\mathtt{t} + 1)(\mathtt{t} + 2) \cdots (\mathtt{t} + k - 1) + k$$

es irreducible en $\mathbb{Z}[\mathtt{t}]$, sus coeficientes son no negativos y, como el producto de k enteros consecutivos es múltiplo de k, su irreducibilidad no puede ser confirmada mediante el Criterio de Cohn ya que para todo entero positivo b mayor que los coeficientes de f se cumple que $f(b) \in k\mathbb{Z}$ no es primo. Sin embargo, la denominada *Conjetura de Bunyakovsky,* que debe su nombre a Viktor Bunyakovsky (1804-1889), matemático ruso que contribuyó en gran medida al desarrollo de la teoría de números, el análisis real y complejo y la probabilidad, va en la línea del resultado que buscamos. La conjetura dice lo siguiente:

Sea $f(\mathtt{t}) \in \mathbb{Z}[\mathtt{t}]$ un polinomio irreducible de grado mayor o igual que 1 con coeficientes enteros y coeficiente director $\ell(f) \geq 1$. Supongamos que existe un entero positivo k de modo que $\operatorname{mcd}(f(1), f(2), \ldots, f(k)) = 1$. *Entonces, existen infinitos enteros no negativos $x_i \in \mathbb{Z}$ tales que $f(x_i)$ es un número primo.*

Esta conjetura no ha sido probada. El caso particular en que $f(\mathtt{t}) := a_0 + a_1\mathtt{t}$ donde $\mathrm{mcd}\,(a_0, a_1) = 1$ fue conjeturado por Gauss y demostrado por Dirichlet.

Aunque el polinomio $f(\mathtt{t}) = \mathtt{t}^2 + \mathtt{t} + 41$ cumple que $f(k)$ es primo para $0 \leq k \leq 39$, Goldbach demostró que no existe ningún polinomio con coeficientes racionales tal que $f(n)$ sea primo para todo $n \in \mathbb{Z}^+$. Mucho más recientemente Jones-Sata-Wada-Wiens encontraron un polinomio f de grado 25 en 26 variables tal que $f(\mathbb{N}^{26}) \cap \mathbb{Z}^+$ es el conjunto de todos los números primos cuando x recorre $\mathbb{N}^{26}$.

Una versión más general de la conjetura de Bunyakovsky afirma que si $f_1, \ldots, f_n \in \mathbb{Z}[\mathtt{t}]$ están en las condiciones de la conjetura y para todo primo p existe $b \in \mathbb{Z}^+$ tal que p no divide a $f_i(b)$ para cada $i = 1, \ldots, n$, entonces existen infinitos enteros positivos m que cumplen que $f_i(m)$ es primo para cada $i = 1, \ldots, n$. Caso de ser probada, esta conjetura demostraría algunas de las conjeturas más famosas de las matemáticas como la *Conjetura de los primos gemelos,* que se corresponde con el caso $f_1(\mathtt{t}) := \mathtt{t}$ y $f_2(\mathtt{t}) := \mathtt{t} + 2$, o la *Conjetura de Sophie-Germain,* que corresponde al caso $f_1(\mathtt{t}) := \mathtt{t}$ y $f_2(\mathtt{t}) := 2\mathtt{t} + 1$.

Observación IV.22 Sea $f \in \mathbb{Z}[\mathtt{t}]$ tal que $\ell(f) \geq 1$ (en caso contrario multiplicamos f por -1). En ocasiones podemos usar la conjetura de Bunyakovsky junto con el Corolario IV.5 para decidir la irreducibilidad de f. En efecto, la conjetura de Bunyakovsky asegura, para un conjunto grande de polinomios f, que existen infinitos enteros n tales que $f(n)$ es primo. Observemos en primer lugar que si el término independiente de un polinomio $f \in \mathbb{Z}[\mathtt{t}]$ cumple que $f(0) = a_0 = \pm 1$, no existe $m > 1$ tal que $m | f(n)$ para todo $n \in \mathbb{N}$. Para ver esto, si denotamos $d := \deg(f)$, escribimos

$$f(\mathtt{t}) = \mathtt{t}g(\mathtt{t}) + a_0$$

donde $g(\mathtt{t})$ es un polinomio de grado $d - 1$. Entonces m no divide a $f(m) = mg(m) \pm 1$ para todo $m \in \mathbb{Z}$ mayor que 1.

Se trata por tanto de transformar, mediante un procedimiento que preserve la irreducibilidad, el polinomio primitivo $f \in \mathbb{Z}[\mathtt{t}]$ cuya irreducibilidad queremos estudiar en otro, digamos g, que cumpla $g(0) = \mathtt{c}(g)$. Si logramos esto, escribimos $g(\mathtt{t}) = \mathtt{c}(g)g_1$ y se tiene $g_1(0) = 1$. La irreducibilidad de g_1 en $\mathbb{Z}[\mathtt{t}]$ se puede abordar mediante la conjetura de Bunyakowsky. Esta implica la irreducibilidad en $\mathbb{Q}[\mathtt{t}]$ de g, y por ello la de f, lo que junto con el hecho de que f es primitivo proporciona su irreducibilidad en $\mathbb{Z}[\mathtt{t}]$.

¿Y cuál es el procedimiento para asociar g a f preservando la irreducibilidad? El Criterio de la homotecia I.8 eligiendo $a := |f(0)|$. A partir de aquí, basta usar la Proposición IV.2 hasta encontrar $2d + 1$ enteros cuyas imágenes por f sean números primos o sus opuestos. Esto, en virtud de la conjetura de Bunyakovsky, siempre debería ser posible (en caso de encontrar un polinomio que no lo cumpla habríamos demostrado la falsedad de la conjetura), por lo que se trata de efectuar suficientes evaluaciones de f en números enteros hasta encontrar $2d + 1$ cuyas imagenes por f sean números primos.

Este método es con frecuencia ineficaz desde el punto de vista computacional. Por ejemplo, el polinomio: $f(\mathtt{t}) = \mathtt{t}^{12} + 488669$, que es irreducible en $\mathbb{Z}[\mathtt{t}]$ en virtud del Criterio de Eisenstein, Corolario III.3, aplicado con el primo $p = 107$, cumple que $f(616980)$ es primo y $f(n)$ es compuesto para todo $n < 616980$.

CAPÍTULO V

Criterio de Perron

La demostración del Criterio de Cohn ha requerido emplear argumentos que involucran polinomios con coeficientes complejos y sus raíces en $\mathbb{C}$. Esto se ha puesto especialmente de manifiesto en la demostración del Lema IV.13 o en el enunciado del Lema IV.10 que es válido para cualquier polinomio con coeficientes complejos. En la prueba del Criterio de Perron profundizamos en la conexión entre polinomios irreducibles y análisis complejo. La prueba se apoya en el Lema V.4, del que daremos dos demostraciones. La segunda se basa en el Teorema de Rouché del análisis complejo, que no demostraremos. Para comenzar, presentamos un criterio similar al de Perron pero cuya demostración es mucho más sencilla.

Proposición V.1 *Sea* $f(\mathtt{t}) = a_0 + a_1\mathtt{t} + \cdots + a_{d-1}\mathtt{t}^{d-1} + a_d\mathtt{t}^d \in \mathbb{Z}[\mathtt{t}]$ *un polinomio de grado* $d \geq 1$ *tal que* $|a_0|$ *es primo o* 1 *y, además,*

$$\sum_{i=1}^{d} |a_i| < |a_0|.$$

Entonces f *es irreducible en* $\mathbb{Z}[\mathtt{t}]$.

Demostración. Veamos que cada raíz $\alpha \in \mathbb{C}$ cumple $|\alpha| > 1$. En caso contrario,

$$|a_0| = \left|\sum_{i=1}^{d} a_i\alpha^i\right| \leq \sum_{i=1}^{d} |a_i| \cdot |\alpha|^i \leq \sum_{i=1}^{d} |a_i|,$$

contra lo supuesto. Supongamos ahora que f es reducible en $\mathbb{Z}[\mathtt{t}]$. Como es primitivo existen $g, h \in \mathbb{Z}[\mathtt{t}]$ de grado mayor o igual que 1 tales que $f = gh$. Entonces

$$|a_0| = |f(0)| = |g(0)| \cdot |h(0)|$$

y, como $|a_0|$ es primo o 1, se tiene $|g(0)| = 1$ o $|h(0)| = 1$. Sin pérdida de generalidad podemos suponer que $|g(0)| = 1$. Sean $\alpha_1, \ldots, \alpha_{\deg(g)}$ las raíces complejas, no necesariamente distintas, de g. Entonces,

$$g(\mathtt{t}) = \ell(g) \prod_{i=1}^{\deg(g)} (\mathtt{t} - \alpha_i) \quad \rightsquigarrow \quad 1 = |g(0)| = |\ell(g)| \cdot \prod_{i=1}^{\deg(g)} |\alpha_i|.$$

Cada α_i es raíz de f por serlo de g luego, por lo ya probado, cada $|\alpha_i| > 1$, así que

$$1 < \prod_{i=1}^{\deg(g)} |\alpha_i| = \frac{1}{|\ell(g)|} \leq 1,$$

que es una contradicción, lo que demuestra que f es irreducible en $\mathbb{Z}[\mathtt{t}]$. □

Ejemplo V.2 El polinomio $f(\mathtt{t}) = \mathtt{t}^4 - 3\mathtt{t}^3 + 3\mathtt{t}^2 - 3\mathtt{t} + 7$ es irreducible en $\mathbb{Z}[\mathtt{t}]$. Empleando el Criterio de la traslación I.7, basta probar que lo es $g(\mathtt{t}) := f(\mathtt{t}+1)$. Como

$$g(\mathtt{t}) = \mathtt{t}^4 + \mathtt{t}^3 - 2\mathtt{t} + 5$$

es suficiente aplicar la Proposición anterior V.1.

Sin más preámbulo, enunciamos el Criterio de Perron.

Teorema V.3 (Criterio de Perron) *Sea* $f(\mathtt{t}) = a_0 + a_1\mathtt{t} + \cdots + a_{d-1}\mathtt{t}^{d-1} + \mathtt{t}^d \in \mathbb{Z}[\mathtt{t}]$ *tal que* $a_0 \neq 0$*, y supongamos que* $|a_0| + \cdots + |a_{d-2}| + 1 < |a_{d-1}|$*. Entonces* f *es irreducible en* $\mathbb{Z}[\mathtt{t}]$

Antes de demostrar este teorema, necesitaremos el siguiente lema previo.

Lema V.4 *Sea* $f(\mathtt{t}) := a_0 + a_1\mathtt{t} + \cdots + a_{d-1}\mathtt{t}^{d-1} + \mathtt{t}^d \in \mathbb{Z}[\mathtt{t}]$ *tal que* $a_0 \neq 0$ *y*

$$|a_0| + \cdots + |a_{d-2}| + 1 < |a_{d-1}|.$$

Entonces, exactamente una de las raíces complejas de f *tiene módulo mayor que* 1 *y, además, su multiplicidad como raíz de* f *es* 1*. Las restantes raíces complejas* $\alpha_2, \ldots, \alpha_d$ *de* f*, no necesariamente distintas, cumplen* $|\alpha_i| < 1$*.*

Demostraremos este lema de dos maneras distintas. En la segunda empleamos uno de los teoremas básicos del análisis complejo: el Teorema de Rouché.

Demostración. En primer lugar veamos, por reducción al absurdo, que ninguna raíz compleja α de f cumple $|\alpha| = 1$. En efecto, sea $\alpha \in \mathbb{C}$ un raíz de f. Entonces,

$$-a_{d-1}\alpha^{d-1} = a_0 + a_1\alpha + \cdots + a_{d-2}\alpha^{d-2} + \alpha^d. \tag{V.1}$$

Supongamos que $|\alpha| = 1$. Tomando módulos en la igualdad (V.1) se tiene

$$|a_{d-1}| = |a_{d-1}\alpha^{d-1}| = |a_0 + a_1\alpha + \cdots + a_{d-2}\alpha^{d-2} + \alpha^d| \leq |a_0| + |a_1| + \cdots + |a_{d-2}| + 1,$$

en contra de lo supuesto en el enunciado. Denotamos $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ las raíces complejas de f, no necesariamente distintas. Como f es mónico se tiene

$$f(\mathtt{t}) = \prod_{i=1}^{d}(\mathtt{t} - \alpha_i) \quad \rightsquigarrow \quad \prod_{i=1}^{d}|\alpha_i| = \left|\prod_{i=1}^{d}\alpha_i\right| = |f(0)| = |a_0| \geq 1,$$

luego al menos una raíz de f, digamos α_1, cumple $|\alpha_1| > 1$. Como $f(\mathtt{t})$ es múltiplo en $\mathbb{C}[\mathtt{t}]$ de $\mathtt{t} - \alpha_1$ se escribe

$$g(\mathtt{t}) := \frac{f(\mathtt{t})}{(\mathtt{t} - \alpha_1)} = b_0 + b_1\mathtt{t} + \cdots + b_{d-1}\mathtt{t}^{d-1} \in \mathbb{C}[\mathtt{t}],$$

o lo que es lo mismo,

$$f(\mathtt{t}) = (\mathtt{t} - \alpha_1)(b_0 + b_1\mathtt{t} + \cdots + b_{d-1}\mathtt{t}^{d-1}) = b_{d-1}\mathtt{t}^d + (b_{d-2} - b_{d-1}\alpha_1)\mathtt{t}^{d-1} + \cdots - b_0\alpha_1. \tag{V.2}$$

Todo se reduce a probar que el módulo de cada raíz de g es menor que 1 pues esto implica, en particular, que α_1 no es raíz de g, es decir, α_1 es raíz simple de f. Igualando coeficientes en la expresión (V.2) y, puesto que f es mónico,

$$b_{d-1} = 1, \quad a_0 = -b_0\alpha_1 \quad \text{y} \quad a_k = b_{k-1} - b_k\alpha_1 \text{ para todo } k = 1, \dots, d-1.$$

Empleando la desigualdad del enunciado y la desigualdad triangular resulta:

$$\begin{aligned} |b_{d-2}| + |\alpha_1| \geq |b_{d-2} - \alpha_1| = |b_{d-2} - b_{d-1}\alpha_1| = |a_{d-1}| > 1 + |a_{d-2}| + \cdots + |a_0| \\ = 1 + |b_{d-3} - b_{d-2}\alpha_1| + \cdots + |b_0 - b_1\alpha_1| + |b_0\alpha_1| \\ \geq 1 + (|b_{d-2}| \cdot |\alpha_1| - |b_{d-3}|) + \cdots + (|b_1| \cdot |\alpha_1| - |b_0|) + |b_0| \cdot |\alpha_1| \\ = 1 + |b_{d-2}| + (|\alpha_1| - 1)\left(|b_{d-2}| + |b_{d-3}| + \cdots + |b_1| + |b_0|\right). \end{aligned}$$

Simplificando el sumando $|b_{d-2}|$ en ambos miembros y pasando el sumando 1 de la derecha a la izquierda se tiene

$$|\alpha_1| - 1 > (|\alpha_1| - 1)\left(|b_{d-2}| + |b_{d-3}| + \cdots + |b_1| + |b_0|\right),$$

y puesto que $|\alpha_1| > 1$ resulta $\sum_{j=0}^{d-2} |b_j| < 1$. Para terminar, supongamos que g posee una raíz α que cumple $|\alpha| > 1$. Entonces:

$$\begin{aligned} 0 = |g(\alpha)| = \left|\sum_{j=0}^{d-2} b_j\alpha^j + \alpha^{d-1}\right| \geq |\alpha|^{d-1} - \sum_{j=1}^{d-2} |b_j| \cdot |\alpha|^j - b_0 \\ \geq |\alpha|^{d-1} - |\alpha|^{d-1}\Big(\sum_{j=0}^{d-2} |b_j|\Big) = \alpha|^{d-1}\Big(1 - (\sum_{j=0}^{d-2} |b_j|\Big) > 0 \end{aligned}$$

que es una contradicción ya que $g(\alpha) = 0$. □

Para la segunda demostración de este lema necesitamos el Teorema de Rouché. Para enunciarlo necesitamos algunas definiciones previas.

Definición V.5 Sea $\mathcal{C} \subset \mathbb{R}^n$ una curva diferenciable compacta. Se dice que $\mathcal{C}$ es una *curva cerrada simple* si existe una aplicación diferenciable $\mathtt{x} : I := [a, b] \to \mathbb{R}^n$ tal que $\mathtt{x}(I) = \mathcal{C}$, $\mathtt{x}(a) = \mathtt{x}(b)$ y la restricción de $\mathtt{x}$ al intervalo abierto (a, b) es inyectiva.

Observación V.6 La circunferencia unidad es una curva cerrada simple, parametrizada por la aplicación $\mathtt{x} : [0, 1] \to \mathbb{R}^2$, $t \mapsto (\cos 2\pi t, \operatorname{sen} 2\pi t)$ que es diferenciable, su restricción al intervalo $(0, 1)$ es inyectiva y cumple $\mathtt{x}(0) = \mathtt{x}(1) = (1, 0)$.

Definiciones V.7 (1) Sea $\Omega \subset \mathbb{C}$ un subconjunto abierto. Se dice que la función $f : \Omega \to \mathbb{C}$ es *analítica* si para cada $z_0 \in \mathbb{C}$ existen un entorno abierto U de z_0 en $\mathbb{C}$ y una serie convergente $\sum_{n=0}^{\infty} a_n\mathtt{t}^n \in \mathbb{C}\{\mathtt{t}\}$ tal que para cada $z \in U$ se tiene

$$f(z) = \sum_{n=0}^{\infty} a_n(z - z_0)^n.$$

(2) Se dice que $z_0 \in \mathbb{C}$ es una raíz de *multiplicidad* k de la función analítica f si $f^{j)}(z_0) = 0$ para $0 \leq j \leq k-1$ y $f^{k)}(z_0) \neq 0$.

Se desprende directamente de la definición que los polinomios en $\mathbb{C}[\mathtt{t}]$ son funciones analíticas de $\mathbb{C}$ en $\mathbb{C}$ y que la multiplicidad de $z_0 \in \mathbb{C}$ como raíz del polinomio f coincide con su multiplicidad como raíz de la función analítica f.

Teorema V.8 (Rouché) *Sean $\Omega \subset \mathbb{C}$ un subconjunto abierto acotado tal que $\mathcal{C} := \overline{\Omega} \setminus \Omega$ es una curva cerrada simple, y g y h dos funciones analíticas en Ω y continuas en $\overline{\Omega}$. Supongamos que $|g(z)| > |h(z)|$ para todo $z \in \mathcal{C}$. Entonces g y $g+h$ tienen el mismo número de raíces en Ω contando cada una tantas veces como indica su multiplicidad.*

Demostración alternativa del Lema V.4. Dado el polinomio $f(\mathtt{t}) := \sum_{i=0}^{d-1} a_i \mathtt{t}^i + \mathtt{t}^d$ del enunciado definimos

$$g(\mathtt{t}) := a_{d-1}\mathtt{t}^{d-1} \quad \text{y} \quad h(\mathtt{t}) := f(\mathtt{t}) - a_{d-1}\mathtt{t}^{d-1}.$$

Consideremos el disco abierto $\Omega := \{z \in \mathbb{C} : |z| < 1\}$ y observamos que, por ser polinomios, las restricciones $g|_\Omega : \Omega \to \mathbb{C}$ y $h|_\Omega : \Omega \to \mathbb{C}$ son funciones analíticas y sus restricciones al disco cerrado $\overline{\Omega}$ son funciones continuas. Nótese que la frontera $\partial\Omega := \overline{\Omega} \setminus \Omega$ es la circunferencia unidad $\mathcal{C} := \{z \in \mathbb{C} : |z| = 1\}$, que es una curva cerrada simple.

Para todo $z \in \mathcal{C}$ se cumple $|z| = 1$ luego, por las hipótesis del enunciado,

$$\begin{aligned} |g(z)| = |a_{d-1}z^{d-1}| = |a_{d-1}| &> 1 + |a_{d-2}| + \cdots + |a_0| \\ = |z^d| + |a_{d-2}| \cdot |z^{d-2}| + \cdots + |a_0| &\geq |z^d + a_{d-2}z^{d-2} + \cdots + a_0| = |h(z)|. \end{aligned} \tag{V.3}$$

Estamos por tanto en las hipótesis del Teorema de Rouché, luego g y $f = g + h$ tienen el mismo número de raíces en Ω. Como g tiene por (única) raíz $\mathtt{t} := 0 \in \Omega$ con multiplicidad $d-1$, f tiene $d-1$ raíces en el interior del disco unidad, como queríamos probar.

Como $\deg(f) = d$, f tiene una única raíz, digamos α, en $\mathbb{C} \setminus \Omega$ y para terminar basta demostrar que $|\alpha| \neq 1$. Para ello basta repetir el argumento empleado en la primera demostración del Lema V.4. Probado éste procedemos a demostrar el Criterio de Perron.

Demostración del Criterio de Perron V.3. Supongamos que f es reducible en $\mathbb{Z}[\mathtt{t}]$. Como es mónico es primitivo, luego si fuese reducible en $\mathbb{Z}[\mathtt{t}]$ existirían polinomios g y h de grado mayor o igual que 1 con coeficientes enteros tales que $f(\mathtt{t}) = g(\mathtt{t})h(\mathtt{t})$. Por el Lema V.4, f tiene sólo una raíz α_1 que cumpla $|\alpha_1| > 1$, y por tanto uno de los polinomios g o h tiene todas sus raíces en el interior del disco unidad. Suponemos sin pérdida de generalidad que ese polinomio es g, cuyas raíces denotamos $\alpha_k, \alpha_{k+1}, \ldots \alpha_d$ para cierto entero $k = 2, \ldots, d$. Entonces:

$$|g(0)| = |\alpha_k \cdots \alpha_d| < 1,$$

que es absurdo ya que $g(0)$ es un entero no nulo. Esto prueba que f es irreducible en $\mathbb{Z}[\mathtt{t}]$.

Ejemplo V.9 El polinomio $f(\mathtt{t}) := \mathtt{t}^6 - \mathtt{t}^5 + 5\mathtt{t} - 1$ es irreducible en $\mathbb{Z}[\mathtt{t}]$. En efecto, por el Lema III.1, f es irreducible en $\mathbb{Z}[\mathtt{t}]$ si y sólo si lo es el polinomio:

$$\widehat{f}(\mathtt{t}) := -\mathtt{t}^6 f(1/\mathtt{t}) = \mathtt{t}^6 - 5\mathtt{t} + \mathtt{t} - 1,$$

cuya irreducibilidad se desprende del Criterio de Perron V.3.

CAPÍTULO VI

Irreducibilidad de los polinomios ciclotómicos

En el Ejemplo III.7 combinamos el Criterio de Eisenstein y el de la traslación para demostrar la irreducibilidad en $\mathbb{Z}[\mathtt{t}]$ del p-ésimo polinomio ciclotómico. En esta sección extendemos este resultado a todos los polinomios ciclotómicos.

Definiciones VI.1 (Raíces de la unidad) (1) Para cada entero positivo n el conjunto

$$\mathcal{U}_n := \{\zeta \in \mathbb{C} : \zeta^n = 1\}$$

es un subgrupo cíclico de orden n del grupo multiplicativo $\mathbb{C}^*$ formado por los números complejos no nulos, llamado *grupo de las raíces n-ésimas de la unidad.* Un generador es $\zeta_n := e^{2\pi \mathtt{i}/n}$.

(2) Se dice que $\zeta \in \mathcal{U}_n$ es una *raíz primitiva* n-ésima de la unidad si $\mathcal{U}_n = \langle\zeta\rangle$, es decir, si el orden $o(\zeta)$ de ζ como elemento de $\mathcal{U}_n$ es n. El número de ellas es $\varphi(n)$, donde $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ es la función de Euler, que hace corresponder a cada entero m el cardinal del conjunto formado por todos los números enteros $k = 1, \ldots, n$ tales que $\operatorname{mcd}(k, n) = 1$.

En efecto como $\mathcal{U}_n = \langle\zeta_n\rangle$, cada raíz n-esima de la unidad ζ es potencia de ζ_n, es decir, $\zeta := \zeta_n^k$ para cierto entero positivo $k = 1, \ldots, n$, y ζ es primitiva si y sólo si

$$n = o(\zeta) = o(\zeta_n^k) = \frac{o(\zeta_n)}{\operatorname{mcd}(k, o(\zeta_n))} = \frac{n}{\operatorname{mcd}(k, n)} \quad \text{es decir} \quad \operatorname{mcd}(k, n) = 1.$$

En lo que sigue denotaremos $\mathcal{P}_n$ el conjunto de raíces primitivas n-ésimas de la unidad.

Definiciones VI.2 (Polinomios ciclotómicos) (1) Para cada $n \geq 1$ se define el n-ésimo *polinomio ciclotómico* como el producto

$$\Phi_n(\mathtt{t}) := \prod_{\zeta \in \mathcal{P}_n} (\mathtt{t} - \zeta) \in \mathbb{C}[\mathtt{t}].$$

Si p es un número primo la única raíz p-ésima de la unidad que no es primitiva es 1, luego

$$\Phi_p(\mathtt{t}) = \prod_{\zeta \in \mathcal{P}_p} (\mathtt{t} - \zeta) = \frac{\mathtt{t}^p - 1}{\mathtt{t} - 1} = \sum_{j=0}^{p-1} \mathtt{t}^j,$$

ya que para cada $\zeta := \zeta_p^k$, con $k = 1, \ldots, p$ se tiene $\zeta^p - 1 = 0$ y, dividiendo por $\mathtt{t} - 1$, eliminamos el factor que corresponde a la raíz $1 = \zeta_p^p$, que es la única que no es primitiva. Esta es la definición de p-ésimo polinomio ciclotómico dada en el Ejemplo III.7

(2) Acabamos de señalar que $\mathrm{Card}(\mathcal{P}_n) = \varphi(n)$, luego Φ_n es un polinomio mónico de grado $\varphi(n)$. Se deduce directamente de la definición que todas las raíces de Φ_n en $\mathbb{C}$ son simples.

(3) Sean $d > 0$ un divisor de n y $\zeta \in \mathcal{U}_n$. Ésta es raíz primitiva d-ésima de la unidad si y sólo si $o(\zeta) = d$, donde $o(\zeta)$ es el orden de ζ como elemento de $\mathcal{U}_n$.

(4) Denotemos $D(n) := \{d \geq 1 : d|n\}$ el conjunto formado por los divisores positivos de n. Por la Fórmula de Lagrange, $o(\zeta) \in D(n)$ para cada $\zeta \in \mathcal{U}_n$. Por tanto, $\mathcal{U}_n = \bigsqcup_{d\in D(n)} \mathcal{P}_d$, es decir, toda raíz n-ésima de la unidad es raíz primitiva d-ésima de la unidad para un único divisor d de n. En consecuencia,

$$\mathtt{t}^n - 1 = \prod_{\zeta\in\mathcal{U}_n} (\mathtt{t} - \zeta) = \prod_{d\in D(n)} \prod_{\zeta\in\mathcal{P}_d} (\mathtt{t} - \zeta) = \prod_{d\in D(n)} \Phi_d(\mathtt{t}). \tag{VI.1}$$

Proposición VI.3 *Para cada entero $n \geq 1$ el polinomio ciclotómico $\Phi_n \in \mathbb{Z}[\mathtt{t}]$, y si $n \geq 2$ su término independiente vale* 1.

Demostración. Probamos por inducción sobre n que $\Phi_n \in \mathbb{Z}[\mathtt{t}]$. Esto es obvio para $n = 1$ pues $\Phi_1(\mathtt{t}) = \mathtt{t} - 1$. Denotamos $D_1(n) := D(n) \setminus \{n\}$ y

$$P_n(\mathtt{t}) := \prod_{d\in D_1(n)} \Phi_d(\mathtt{t}).$$

Por la hipótesis de inducción, $\Phi_d \in \mathbb{Z}[\mathtt{t}]$ para cada $d \in D_1(n)$, luego $P_n \in \mathbb{Z}[\mathtt{t}]$ y rescribimos (VI.1):

$$\mathtt{t}^n - 1 = \prod_{d\in D(n)} \Phi_d(\mathtt{t}) = \Phi_n(\mathtt{t}) \cdot \prod_{d\in D_1(n)} \Phi_d(\mathtt{t}) = \Phi_n(\mathtt{t}) \cdot P_n(\mathtt{t}). \tag{VI.2}$$

Como $P_n \in \mathbb{Z}[\mathtt{t}]$ y es mónico por serlo cada polinomio ciclotómico, se puede dividir $\mathtt{t}^n - 1$ entre $P_n(\mathtt{t})$ en $\mathbb{Z}[\mathtt{t}]$. Esto significa que existen $q, r \in \mathbb{Z}[\mathtt{t}]$ tales que $\deg(r) < \deg(P_n)$ y $\mathtt{t}^n - 1 = P_n(\mathtt{t}) \cdot q(\mathtt{t}) + r(\mathtt{t})$. Esta igualdad es también una división euclídea en el dominio euclídeo $\mathbb{C}[\mathtt{t}]$, pero tamnbién lo es $\mathtt{t}^n - 1 = P_n(\mathtt{t}) \cdot \Phi_n(\mathtt{t}) + 0$. Por la unicidad del cociente y el resto, deducimos que $r = 0$ y $\Phi_n = q \in \mathbb{Z}[\mathtt{t}]$.

También empleamos inducción para probar que $\Phi_n(0) = 1$. El caso $n = 2$ es obvio pues $\Phi_2(\mathtt{t}) = \mathtt{t} + 1$. Suponemos el resultado probado para cada entero m con $2 \leq m < n$ y escribimos la igualdad (VI.2) como

$$\mathtt{t}^n - 1 = \prod_{d\in D(n)} \Phi_d(\mathtt{t}) = (\mathtt{t} - 1) \cdot \Phi_n(\mathtt{t}) \cdot \prod_{d\in D_2(n)} \Phi_d(\mathtt{t}), \tag{VI.3}$$

donde $D_2(n) := D_1(n)\setminus\{1\}$. Por hipótesis de inducción $\Phi_d(0) = 1$ para cada $d \in D_2(n)$, así que evaluando en $\mathtt{t} = 0$ los dos miembros de la igualdad (VI.3) se tiene $-1 = (-1)\cdot\Phi_n(0)\cdot 1$, es decir, $\Phi_n(0) = 1$. □

Teorema VI.4 *El polinomio ciclotómico $\Phi_n \in \mathbb{Z}[\mathtt{t}]$ es irreducible en $\mathbb{Z}[\mathtt{t}]$.*

Demostración. Supongamos que Φ_n es reducible en $\mathbb{Z}[\mathtt{t}]$. Por ser mónico, Φ_n es primitivo, luego existen $f, g \in \mathbb{Z}[\mathtt{t}]$ mónicos de grado mayor o igual que 1 tales que f es irreducible en $\mathbb{Z}[\mathtt{t}]$ y $\Phi_n = fg$. Así f es irreducible en $\mathbb{Q}[\mathtt{t}]$ y tomamos una raíz ζ de f en $\mathbb{C}$. Probemos:

Si un número primo p no divide a n, y $\xi \in \mathbb{C}$ es raíz de f, entonces ξ^p es también raíz de f.

En efecto, supongamos que $f(\xi^p) \neq 0$. Obsérvese que ξ^p es raíz primitiva n-ésima de la unidad, ya que $(\xi^p)^n = (\xi^n)^p = 1$ y

$$o(\xi^p) = \frac{o(\xi)}{\operatorname{mcd}(p, o(\xi))} = \frac{n}{\operatorname{mcd}(p,n)} = \frac{n}{1} = n.$$

Esto implica que $\Phi_n(\xi^p) = 0$, luego $g(\xi^p) = 0$. Sea $h(\mathtt{t}) := g(\mathtt{t}^p) \in \mathbb{Z}[\mathtt{t}]$. Como f es mónico se puede dividir h entre f en $\mathbb{Z}[\mathtt{t}]$ y existen un cociente $q \in \mathbb{Z}[\mathtt{t}]$ y un resto $r \in \mathbb{Z}[\mathtt{t}]$ tales que $h = fq + r$ y $\deg(r) < \deg(f)$. Ésta es también una división en el dominio euclídeo $\mathbb{Q}[\mathtt{t}]$. Pero, como f es el polinomio mínimo de ξ en $\mathbb{Q}[\mathtt{t}]$, por ser irreducible y tener a ξ por raíz, y $h(\xi) = g(\xi^p) = 0$, el polinomio h es múltiplo en $\mathbb{Q}[\mathtt{t}]$ de f. Por la unicidad de la división, $r = 0$, luego $q \in \mathbb{Z}[\mathtt{t}]$ y $h = fq$.

El homomorfismo sobreyectivo $\mathbb{Z} \to \mathbb{Z}_p,\ x \to [x]_p := x + p\mathbb{Z}$ induce otro, llamado *reducción* $\bmod p$,

$$\Psi : \mathbb{Z}[\mathtt{t}] \to \mathbb{Z}_p[\mathtt{t}],\ \sum_{k=0}^{m} a_k \mathtt{t}^k \mapsto \sum_{k=0}^{m} [a_k]_p \mathtt{t}^k.$$

Escribimos $g(\mathtt{t}) := \sum_{j=0}^{\ell} b_j \mathtt{t}^j$, por lo que $h(\mathtt{t}) = \sum_{j=0}^{\ell} b_j \mathtt{t}^{jp}$. Para $0 \leq j \leq \ell$ se cumple, por el Pequeño Teorema de Fermat, la igualdad $[b_j]_p^p = [b_j]_p$, luego

$$\Psi(g)^p = \Big(\sum_{j=0}^{\ell} [b_j]_p \mathtt{t}^j \Big)^p = \sum_{j=0}^{\ell} [b_j]_p^p \mathtt{t}^{jp} = \sum_{j=0}^{\ell} [b_j]_p \mathtt{t}^{jp} = \Psi(h).$$

Por tanto,

$$\Psi(f) \cdot \Psi(q) = \Psi(fq) = \Psi(h) = \Psi(g)^p.$$

Sea $q_1 \in \mathbb{Z}[\mathtt{t}]$ cuya imagen $\Psi(q_1)$ es un factor irreducible de $\Psi(f)$ en $\mathbb{Z}_p[\mathtt{t}]$. Como $\Psi(f)$ divide a $\Psi(h) = \Psi(g)^p$ se deduce que $\Psi(q_1)$ divide a $\Psi(g)^p$, por lo que $\Psi(q_1) | \Psi(g)$. Esto implica que $\Psi(q_1)^2$ divide a $\Psi(f) \cdot \Psi(g) = \Psi(\Phi_n)$, que a su vez divide a $\Psi(\mathtt{t}^n - 1)$. Por tanto, $\Psi(\mathtt{t}^n - 1) = \Psi(\mathtt{t})^n - 1$ tiene un factor múltiple, o lo que es lo mismo, $\Psi(\mathtt{t}^n - 1)$ y su derivada $n\Psi(\mathtt{t})^{n-1}$ tienen un factor en común. Como p y n son primos entre sí el polinomio $n\Psi(\mathtt{t})^{n-1}$ es no nulo y su único factor irreducible en $\mathbb{Z}[\mathtt{t}]$ es $\Psi(\mathtt{t})$. Por tanto, $\Psi(\mathtt{t})$ ha de dividir a $\Psi(\mathtt{t})^n - 1$, lo cual es falso. En consecuencia, ξ^p no es raíz de g, luego lo es de f, como pretendíamos demostrar.

Como $\deg(g) \geq 1$ existe $\eta \in \mathbb{C}$ tal que $g(\eta) = 0$, luego $\Phi_n(\eta) = 0$ y η es una raíz primitiva n-ésima de la unidad. Por ello existe un entero $s \geq 1$ primo con n tal que $\eta = \zeta^s$. Escribimos $s = p_1 \cdots p_\ell$, donde cada p_i es un número primo que no divide a n. Como ζ es raíz de f se deduce de lo que acabamos de probar que ζ^{p_1} es también raíz de f y, reiterando el proceso, resulta que $\eta = \zeta^{p_1 \cdots p_\ell}$ es raíz de f. Por tanto, f y g comparten una raíz, lo que significa que el polinomio ciclotómico Φ_n tiene una raíz múltiple en $\mathbb{C}$, y esto contradice VI.2 (2). Concluimos así que Φ_n es irreducible en $\mathbb{Z}[\mathtt{t}]$. □

CAPÍTULO VII

Irreducibilidad de curvas planas

Definición VII.1 Para nosotros una *curva plana* sobre un cuerpo K es un polinomio $f \in K[\mathtt{x},\mathtt{y}]$ en dos variables.

Como $A := K[\mathtt{x}]$ es un DFU, los criterios estudiados en este trabajo en todas sus secciones, salvo la quinta dedicada a los polinomios con coeficientes enteros, son aplicables en este contexto. Veamos algún ejemplo.

Ejemplos VII.2 (1) La curva plana $f \in K[\mathtt{x},\mathtt{y}]$, donde

$$f := \mathtt{x}^2\mathtt{y}^5 + \mathtt{x}^3 + \mathtt{x}\mathtt{y}^2 + \mathtt{y}^2 + \mathtt{x} - 1,$$

es irreducible. Denotamos $A := K[\mathtt{y}]$, que es un DFU, y escribimos f como polinomio mónico en el anillo $A[\mathtt{x}] = K[\mathtt{x},\mathtt{y}]$, esto es,

$$f = \mathtt{x}^3 + \mathtt{y}^5\mathtt{x}^2 + (1+\mathtt{y}^2)\mathtt{x} + (\mathtt{y}^2 - 1).$$

Como f es mónico y $\deg_{\mathtt{x}}(f) = 3$, para probar la irreduciblidad de f en $A[\mathtt{x}]$ es suficiente, en virtud de la Proposición I.5, comprobar que f no tiene raíces en A. Las posibles raíces de f en A son divisores en A de su término independiente $\mathtt{y}^2 - 1 = (\mathtt{y}-1)(\mathtt{y}+1)$, es decir, son de la forma $c, c\,(\mathtt{y}+\varepsilon)$ o $c\,(\mathtt{y}^2-1)$, donde $c \in K \setminus \{0\}$ y $\varepsilon = \pm 1$. Al evaluar f en $\mathtt{x} := c$ se obtiene

$$f(c) = c^2\mathtt{y}^5 + (c+1)\mathtt{y}^2 + (c^3 + c - 1) \neq 0,$$

mientras que al evaluar f en $\mathtt{x} := c\,(\mathtt{y}+\varepsilon)$ y en $\mathtt{x} := c\,(\mathtt{y}^2-1)$ existen polinomios $h_1, h_2 \in A$ con $\deg(h_1) < 7$ y $\deg(h_2) < 9$ tales que

$$f\big(c\,(\mathtt{y}+\varepsilon)\big) = c^2\mathtt{y}^7 + h_1 \neq 0 \quad \text{y} \quad f_1\big(c\,(\mathtt{y}^2-1)\big) = c^2\mathtt{y}^9 + h_2 \neq 0.$$

(2) La curva plana $g := \mathtt{x}^2\mathtt{y}^5 + \mathtt{y}\mathtt{x}^3 - \mathtt{x}^2\mathtt{y}^2 + \mathtt{y} - 1 \in K[\mathtt{x},\mathtt{y}]$ es irreducible. Para verlo reescribimos $g = a_3(\mathtt{y})\mathtt{x}^3 + a_2(\mathtt{y})\mathtt{x}^2 + a_0(\mathtt{y})$ donde

$$a_3(\mathtt{y}) := \mathtt{y},\ \ a_2(\mathtt{y}) := \mathtt{y}^5 - \mathtt{y}^2 = \mathtt{y}^2(\mathtt{y}^3-1) = \mathtt{y}^2(\mathtt{y}-1)(\mathtt{y}^2+\mathtt{y}+1)\ \text{ y }\ a_0(\mathtt{y}) := \mathtt{y} - 1.$$

El polinomio $a_0(\mathtt{y}) := \mathtt{y} - 1$ es irreducible en el dominio de factorización única $A := K[\mathtt{y}]$ y divide a a_2 pero $a_0^2 \nmid a_0$. Además g es primitivo, pues $\mathrm{mcd}_A(a_0, a_3) = 1$, luego g es irreducible en $A[\mathtt{x}] = \mathbb{C}[\mathtt{x},\mathtt{y}]$ por el Criterio de Eisenstein.

(3) La curva plana $h \in \mathbb{R}[\mathtt{x},\mathtt{y}]$, donde

$$h := -\mathtt{x} + \mathtt{y} + \mathtt{x}^2 + \mathtt{x}\mathtt{y} + \mathtt{x}^2\mathtt{y} + \mathtt{x}^2\mathtt{y}^2 + \mathtt{x}^2\mathtt{y}^3 + \mathtt{x}^2\mathtt{y}^4,$$

es irreducible. Para probarlo aplicamos el Criterio modular, II.2. Escribimos $\mathbb{R}[\mathtt{x},\mathtt{y}] := A[\mathtt{x}]$, donde $A := \mathbb{R}[\mathtt{y}]$, y denotamos $\mathfrak{p} := (\mathtt{y}-1)A$, que es un ideal primo de A porque, al ser de grado 1, el polinomio $\mathtt{y}-1$ es irreducible en A. El polinomio

$$h = (\mathtt{y}^4+\mathtt{y}^3+\mathtt{y}^2+\mathtt{y}+1)\mathtt{x}^2+(\mathtt{y}-1)\mathtt{x}+\mathtt{y} \in A[\mathtt{x}]$$

es primitivo, ya que $\operatorname{mcd}(\mathtt{y}-1,\mathtt{y})=1$. Para calcular la reducción $\bmod \mathfrak{p}$ de h observamos que $\mathtt{y} \equiv 1 \bmod \mathfrak{p}$, mientras que, por la Regla de Ruffini,

$$p(\mathtt{y}) := \mathtt{y}^4+\mathtt{y}^3+\mathtt{y}^2+\mathtt{y}+1 \equiv p(1) = 5 \bmod \mathfrak{p}.$$

Por tanto, la reducción $\bmod \mathfrak{p}$ de f es $\overline{f} = 5\mathtt{x}^2+1 \in (A/\mathfrak{p})[\mathtt{x}] \simeq \mathbb{R}[\mathtt{x}]$, que es irreducible en $\mathbb{R}[\mathtt{x}]$ pues tiene grado 2 y carece de raíces en $\mathbb{R}$. Esto implica que f es irreducible en $\mathbb{R}[\mathtt{x},\mathtt{y}]$.

(4) Sea $g \in \mathbb{R}[\mathtt{x}]$ un polinomio no nulo tal que $g(x) \geq 0$ para cada $x \in \mathbb{R}$. Comprobemos que la curva plana $f := \mathtt{y}^2+g \in \mathbb{R}[\mathtt{x},\mathtt{y}]$ es irreducible.

Sea $A := \mathbb{R}[\mathtt{x}]$. Si f fuese reducible en $A[\mathtt{y}]$, y puesto que $\deg_{\mathtt{y}}(f)=2$ y f es mónico como polinomio en $A[\mathtt{y}]$, existirían polinomios f_1 y f_2 en $A[\mathtt{y}]$, mónicos y de grado 1 respecto de $\mathtt{y}$, tales que $f = f_1 f_2$. Existirían, por tanto, $g_1, g_2 \in \mathbb{R}[\mathtt{x}]$ tales que $f_i := \mathtt{y}+g_i$ para $i=1,2$, luego

$$\mathtt{y}^2+g = f := f_1 f_2 = (\mathtt{y}+g_1)(\mathtt{y}+g_2) = \mathtt{y}^2+(g_1+g_2)\mathtt{y}+g_1 g_2,$$

por lo que $g_1+g_2=0$ y $g = g_1 g_2 = -g_1^2$. Así, $0 \leq g(x) = -g_1^2(x) \leq 0$, esto es, $g(x)=0$ para cada $x \in \mathbb{R}$. Eso significa que g sería el polinomio nulo, contra lo supuesto.

Disponemos también de criterios específicos del estudio de la irreducibilidad de curvas planas.

Proposición VII.3 (Criterio de Gibson) *Sean K un cuerpo y $f_1, f_2 \in K[\mathtt{x},\mathtt{y}]$ dos polinomios homogéneos primos entre sí de grados $d \geq 1$ y $d+1$, respectivamente. Entonces el polinomio $f := f_1+f_2$ es irreducible en $K[\mathtt{x},\mathtt{y}]$.*

Demostración. Supongamos que existen $g, h \in K[\mathtt{x},\mathtt{y}]$ de grado total al menos 1 tales que $f = gh$. Escribimos g y h como suma de sus componentes homogéneas,

$$g = g_k + \cdots + g_\ell \quad \text{y} \quad h = h_r + \cdots + h_s,$$

con $k \leq \ell$ y $r \leq s$, donde cada g_i y cada h_i es, o bien nulo, o bien un polinomio homogéneo de $K[\mathtt{x},\mathtt{y}]$ de grado total i. Además, g_k, g_ℓ, h_r y h_s son no nulos, y por ello $g_k \neq g_\ell$ si $k \neq \ell$ y $h_r \neq h_s$ si $r \neq s$. Cada producto $g_i h_j$ es nulo o un polinomio homogéneo de grado $i+j$. Por tanto, la componente homogénea de menor grado de $f = gh$ es $g_k h_r$ y la de mayor grado es $g_\ell h_s$. A fortiori son las únicas, pues f tiene, exactamente, dos componentes homogéneas, que son f_1, la de grado menor, y f_2 la de grado mayor. Así $f_1 = g_k h_r$ y $f_2 = g_\ell h_s$, lo que implica que

$$\begin{aligned} 1 = (d+1)-d = \deg(f_2)-\deg(f_1) &= \deg(g_\ell h_s)-\deg(g_k h_r) \\ &= (\ell+s)-(k+r) = (\ell-k)+(s-r), \end{aligned}$$

luego $k = \ell$ o $r = s$. Podemos suponer sin pérdida de generalidad lo primero, así que $f_1 = g_k h_r$ y $f_2 = g_k h_s$, por lo que g_k, cuyo grado es al menos 1, divide a f_1 y a f_2. Esto contradice el hecho de que f_1 y f_2 son primos entre sí. □

Ejemplo VII.4 Aplicamos a continuación la Proposición VII.3 para demostrar que la curva plana $f := \mathtt{x}^3 + \mathtt{x}^2\mathtt{y} - 2\mathtt{x}\mathtt{y}^2 + 3\mathtt{x}\mathtt{y}^3 + 3\mathtt{y}^4 \in K[\mathtt{x}, \mathtt{y}]$ es irreducible.

Escribimos $f := g + h$ donde $g := \mathtt{x}^3 + \mathtt{x}^2\mathtt{y} - 2\mathtt{x}\mathtt{y}^2$ es un polinomio homogéneo de grado 3 y $h := 3\mathtt{x}\mathtt{y}^3 + 3\mathtt{y}^4$ es homogéneo de grado 4. Para probar que f es irreducible en $K[\mathtt{x}, \mathtt{y}]$ es suficiente demostrar, en virtud de la Proposición VII.3, que $\operatorname{mcd}(g, h) = 1$. Para ello factorizamos g y h como producto de factores irreducibles. Se tiene

$$h = 3(\mathtt{x} + \mathtt{y})\mathtt{y}^3 \quad \text{y} \quad g = \mathtt{x}(\mathtt{x}^2 + \mathtt{x}\mathtt{y} - 2\mathtt{y}^2).$$

Para factorizar $\mathtt{x}^2 + \mathtt{x}\mathtt{y} - 2\mathtt{y}^2$ introducimos la variable auxiliar $\mathtt{t} := \frac{\mathtt{x}}{\mathtt{y}}$ y, empleando la Regla de Ruffini,

$$\begin{aligned} \mathtt{x}^2 + \mathtt{x}\mathtt{y} - 2\mathtt{y}^2 &= \mathtt{t}^2\mathtt{y}^2 + \mathtt{t}\mathtt{y}^2 - 2\mathtt{y}^2 = \mathtt{y}^2(\mathtt{t}^2 + \mathtt{t} - 2) = \mathtt{y}^2(\mathtt{t} - 1)(\mathtt{t} + 2) \\ &= (\mathtt{y}\mathtt{t} - \mathtt{y})(\mathtt{y}\mathtt{t} + 2\mathtt{y}) = (\mathtt{x} - \mathtt{y})(\mathtt{x} + 2\mathtt{y}), \end{aligned}$$

y por tanto $g = \mathtt{x}(\mathtt{x} - \mathtt{y})(\mathtt{x} + 2\mathtt{y})$. En consecuencia g y h no comparten ningún factor irreducible, luego $\operatorname{mcd}(g, h) = 1$, como queríamos comprobar.

Nuestro siguiente objetivo es demostrar un criterio de irreducibilidad, Teorema VII.7, que se atribuye a Lenstra. Antes necesitamos introducir la noción de *índice* de una clase particular de curvas planas y un lema auxiliar.

Definición VII.5 Sean $a_0 \in K$ no nulo, $a_1, \ldots, a_d \in K[\mathtt{x}]$ y la curva plana

$$f := a_0\mathtt{y}^d + a_1(\mathtt{x})\mathtt{y}^{d-1} + \cdots + a_d(\mathtt{x}) \in K[\mathtt{x}, \mathtt{y}]. \tag{VII.1}$$

Se define el *índice* de f como el número racional

$$\mu(f) := \operatorname{máx}\left\{ \frac{\deg(a_i)}{i} : i = 1, \ldots, d \right\}.$$

Lema VII.6 *Sea $f \in K[\mathtt{x}, \mathtt{y}]$ como en* (VII.1)*, y sean $g, h \in K[\mathtt{x}, \mathtt{y}] \setminus K$ tales que $f = gh$. Entonces,*

(1) *Las curvas planas g y h tienen la forma de* (VII.1)

(2) $\mu(f) = \operatorname{máx}\{\mu(g), \mu(h)\}$.

Demostración. (1) Escribimos g y h como polinomios en $A[\mathtt{y}]$, donde $A := K[\mathtt{x}]$, esto es,

$$g := b_0\mathtt{y}^m + b_1(\mathtt{x})\mathtt{y}^{m-1} + \cdots + b_m(\mathtt{x}) \quad \text{y} \quad h := c_0\mathtt{y}^n + c_1(\mathtt{x})\mathtt{y}^{n-1} + \cdots + c_n(\mathtt{x}),$$

donde cada $b_i, c_j \in A$ y, como $b_0 c_0 = a_0 \in K \setminus \{0\}$ se deduce que $b_0, c_0 \in K \setminus \{0\}$, es decir, g y h están en las condiciones de (VII.1).

(2) Obsérvese que $m, n \geq 1$ ya que $g, h \notin K$. Además,

$$d = \deg_{\mathtt{y}}(f) = \deg_{\mathtt{y}}(gh) = \deg_{\mathtt{y}}(g) + \deg_{\mathtt{y}}(h) = m + n,$$

luego $m, n < d$. Además, para cada $i = 1, \ldots, d$ se tiene

$$a_i(\mathtt{x}) = \sum_{j+k=i} b_j(\mathtt{x}) c_k(\mathtt{x}) \tag{VII.2}$$

y, por la definición de índice, $\deg(b_j) \leq j\mu(g)$ y $\deg(c_k) \leq k\mu(h)$.

Denotando $\mu := \max\{\mu(g), \mu(h)\}$ resulta,

$$\begin{aligned} \deg(a_i) &\leq \max\{\deg(b_j c_k) : j + k = i\} \leq \max\{\deg(b_j) + \deg(c_k) : j + k = i\} \\ &\leq \max\{j\mu(g) + k\mu(h) : j + k = i\} \leq \max\{j\mu + k\mu : j + k = i\} = i\mu, \end{aligned} \tag{VII.3}$$

y en consecuencia,

$$\mu(f) := \max\left\{\frac{\deg(a_i)}{i} : 1 \leq i \leq d\right\} \leq \max\left\{\frac{i\mu}{i} : 1 \leq i \leq d\right\} = \mu = \max\{\mu(g), \mu(h)\}.$$

Se trata ahora de probar la desigualdad $\max\{\mu(g), \mu(h)\} \leq \mu(f)$ para lo que basta, por simetría, demostrar que para cada $j = 1, \ldots, m$ se cumple $\deg(b_j) \leq j\rho$, donde $\rho := \mu(f)$.

Escribimos el número racional ρ como cociente $\rho := \frac{p}{q}$ donde p y q son enteros positivos. De la igualdad $f = gh$ se desprende

$$f(\mathtt{x}^q, \mathtt{z}^p) = g(\mathtt{x}^q, \mathtt{z}^p) h(\mathtt{x}^q, \mathtt{z}^p), \tag{VII.4}$$

donde $f(\mathtt{x}^q, \mathtt{z}^p) := a_0 \mathtt{z}^{pd} + a_1(\mathtt{x}^q)\mathtt{z}^{p(d-1)} + \cdots + a_d(\mathtt{x}^q)$,

$$\begin{aligned} g(\mathtt{x}^q, \mathtt{z}^p) &:= b_0 \mathtt{z}^{mp} + b_1(\mathtt{x}^q)\mathtt{z}^{p(m-1)} + \cdots + b_m(\mathtt{x}^q) \quad \text{y} \\ h(\mathtt{x}^q, \mathtt{z}^p) &:= c_0 \mathtt{z}^{np} + c_1(\mathtt{x}^q)\mathtt{z}^{p(n-1)} + \cdots + c_n(\mathtt{x}^q). \end{aligned}$$

El grado total de cada monomio $a_i(\mathtt{x}^q)\mathtt{z}^{p(d-i)}$ de $f(\mathtt{x}^p, \mathtt{z}^p)$ es

$$q\deg(a_i) + p(d-i) \leq qi\mu(f) + p(d-i) = \rho q i + p(d-i) = pi + p(d-i) = pd,$$

y el del monomio $a_0 \mathtt{z}^{pd}$ es exactamente pd. Como éste no se cancela con los demás pues en él no aparece la variable $\mathtt{x}$ resulta que $\deg f(\mathtt{x}^q, \mathtt{z}^p) = pd$.

Por otro lado, $\deg g(\mathtt{x}^q, \mathtt{z}^p) \geq \deg b_0 \mathtt{z}^{mp} = mp$ y, de igual modo, $\deg h(\mathtt{x}^q, \mathtt{z}^p) \geq np$. Ahora, empleando (VII.4) se tiene

$$\begin{aligned} pd = \deg f(\mathtt{x}^q, \mathtt{z}^p) &= \deg\big(g(\mathtt{x}^q, \mathtt{z}^p) h(\mathtt{x}^q, \mathtt{z}^p)\big) = \deg g(\mathtt{x}^q, \mathtt{z}^p) + \deg h(\mathtt{x}^q, \mathtt{z}^p) \\ &\geq mp + np = p(m+n) = pd, \end{aligned} \tag{VII.5}$$

de donde deducimos que $\deg g(\mathtt{x}^q, \mathtt{z}^p) = mp$ y $\deg h(\mathtt{x}^q, \mathtt{z}^p) = np$. Así, para $j = 1, \ldots, m$ resulta

$$mp = \deg g(\mathtt{x}^q, \mathtt{z}^p) \geq \deg b_j(\mathtt{x}^q)\mathtt{z}^{p(m-j)} = q\deg(b_j) + p(m-j),$$

o sea, $q\deg(b_j) \leq pj$, esto es, $\frac{\deg(b_j)}{j} \leq \frac{p}{q} = \rho$, de donde $\deg(b_j) \leq j\rho$, como queríamos probar. □

Teorema VII.7 (Criterio de Lenstra) *Sean $a_0 \in K$ no nulo, $a_1, \ldots, a_d \in K[\mathtt{x}]$ y la curva plana*

$$f := a_0\mathtt{y}^d + a_1(\mathtt{x})\mathtt{y}^{d-1} + \cdots + a_d(\mathtt{x}) \in K[\mathtt{x}, \mathtt{y}]. \tag{VII.6}$$

Denotemos $D := \deg(a_d)$ y supongamos que $\mathrm{mcd}(d, D) = 1$ y que $d\deg(a_i) < iD$ para cada $i = 1, \ldots, d-1$. Entonces, la curva f es irreducible.

Demostración. El polinomio f es primitivo en $A[\mathtt{y}]$ porque a_0 es unidad en A. Por tanto, si fuese reducible en $K[\mathtt{x}, \mathtt{y}]$, existirían $g, h \in K[\mathtt{x}, \mathtt{y}] \setminus K$ tales que $f = gh$. Por hipótesis,

$$\frac{\deg(a_i)}{i} < \frac{D}{d} = \frac{\deg(a_d)}{d},$$

para $i = 1, \ldots, d-1$, luego $\mu(f) = \frac{D}{d}$.

Denotemos $\mu(g) := \frac{\alpha}{\beta}$ y $\mu(h) := \frac{\gamma}{\delta}$, donde $\alpha, \beta, \gamma, \delta \in \mathbb{Z}^+$ y $\mathrm{mcd}\,(\alpha, \beta) = \mathrm{mcd}\,(\gamma, \delta) = 1$. De la definición de índice se desprende que los denominadores β y δ son menores o iguales que los grados, respectivamente, de g y h, luego ambos son menores que $\deg(f) = d$. En virtud del Lema anterior VII.7,

$$\frac{D}{d} = \mu(f) = \mathrm{máx}\,\{\mu(g), \mu(h)\} = \mathrm{máx}\left\{\frac{\alpha}{\beta}, \frac{\gamma}{\delta}\right\},$$

y esta igualdad no puede darse ya que $\mathrm{mcd}\,(D, d) = 1$ y $\beta, \delta < d$. □

Ejemplo VII.8 Vamos a comprobar que la curva plana

$$f(\mathtt{x}, \mathtt{y}) := 2\mathtt{y}^3 - \mathtt{x}\mathtt{y}^2 + 4\mathtt{y}^2 + \mathtt{y}\mathtt{x}^2 + 3\mathtt{x}\mathtt{y} + \mathtt{y} + \mathtt{x}^5 \in \mathbb{C}[\mathtt{x}, \mathtt{y}]$$

es irreducible viendo que se encuentra en las hipótesis del Teorema VII.7. Para ello escribimos f en la forma (VII.1):

$$f(\mathtt{x}, \mathtt{y}) := 2\mathtt{y}^3 + (4 - \mathtt{x})\mathtt{y}^2 + (\mathtt{x}^2 + 3\mathtt{x} + 1)\mathtt{y} + \mathtt{x}^5$$

luego, con las notaciones del Teorema VII.7, $d = 3$, $D = 5$, que son primos entre sí, mientras que $\deg(a_1) = 1$ y $\deg(a_2) = 2$, luego $d\deg(a_i) < iD$ para $i = 1, 2$.

Bibliografía

[A] E. Arrondo: Apuntes de estructuras algebraicas. Notas publicadas online. (2011).

[AG] E. Arrondo, D. Gómez: Apuntes de curvas algebraicas. Notas publicadas online. (2013).

[BBZ] A.I. Bonciocat, N.C. Bonciocat, A. Zaharescu: On the irreducibility of polynomials that take a prime power value. *Bull. Math. Soc. Sci. Math. Roumanie* **54**, 102, (2011), 41-54.

[BFO] J. Brillhart, M. Filaseta, A. Odlyzko: On an irreducibility theorem of A. Cohn. *Canadian J. of Math.* **33** (1981), no. 5, 1055-1059.

[FG] J.F. Fernando, J.M. Gamboa: Estructuras Algebraicas: Divisibilidad en anillos conmutativos. Editorial Sanz y Torres. Segunda edición, (2017).

[G] C.G. Gibson: Elementary Geometry of algebraic curves: An undergraduate Introduction, Cambridge Univ. Press, (1998).

[JSWW] J.P Jones, D. Sato, H. Wada, D. Wiens: Diophantine representation of thebset of prime numbers. *Amer. Math. Montly* **83** (1976), no. 6, 449-464.

[OR] J.J. O'Connor, E.F. Robertson, *Viktor Bunyakovsky,* MacTutor History of Mathematics archive, Univ. St. Andrews.

[PS] G. Pólya, G. Szego: Aufgaben und Lehrsätze aus der Analysis. Springer-Verlag, Berlin, (1964).