Capítulo 5
Factorización de polinomios

El primer objetivo de este capítulo es el siguiente resultado de Gauss: *si A es un dominio de factorización única, entonces el anillo de polinomios $A[X]$ es también un dominio de factorización única*. Después de probarlo, veremos un par de criterios de irreducibilidad de polinomios y como una aplicación probaremos la irreducibilidad de los polinomios ciclotómicos $\Phi_n \in \mathbb{Z}[X]$ introducidos en el capítulo 2.

5.1 Cadenas de ideales principales en $A[X]$

Para empezar nuestra prueba del teorema de Gauss, recordemos que en el capítulo 3 hemos visto que la condición de factorización única es equivalente a las siguientes dos propiedades:

a) toda cadena ascendente de ideales principales

$$(f_1) \subseteq (f_2) \subseteq (f_3) \subseteq \cdots \subseteq A[X]$$

se estabiliza: existe n tal que $(f_n) = (f_{n+1}) = \cdots$;

b) todo polinomio irreducible en $A[X]$ es primo.

Primero, es fácil verificar la propiedad a).

5.1.1. Lema. *Si en A toda cadena ascendente de ideales principales*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots \subseteq A$$

se estabiliza, entonces toda cadena ascendente de ideales principales en el anillo de polinomios $A[X]$

$$(f_1) \subseteq (f_2) \subseteq (f_3) \subseteq \cdots \subseteq A[X]$$

se estabiliza.

Demostración. Una cadena de ideales principales en $A[X]$ es equivalente a una cadena de relaciones de divisibilidad

$$\cdots \mid f_3 \mid f_2 \mid f_1.$$

1) En particular, tenemos

$$\deg f_1 \geq \deg f_2 \geq \deg f_3 \geq \cdots$$

Entonces, para n suficientemente grande se tiene necesariamente $\deg f_n = \deg f_{n+1}$. Dado que $f_{n+1} \mid f_n$, esto implica que $f_n = c_n f_{n+1}$ para alguna constante $c_n \in A$.

2) Denotemos por a_n el coeficiente mayor del polinomio f_n. Tenemos

$$\cdots \mid a_3 \mid a_2 \mid a_1,$$

y por nuestra hipótesis se tiene $a_{n+1} \sim a_n$ para n suficientemente grande.

Las observaciones en 1) y 2) implican que $f_{n+1} \sim f_n$ para n suficientemente grande. ■

La propiedad b) requiere más trabajo que haremos en la siguiente sección.

5.2 Contenido y el lema de Gauss

La idea principal de nuestra prueba consiste en trabajar con el anillo de polinomios más grande

$$K[X], \text{ donde } K := \operatorname{Frac} A.$$

Este es un dominio de ideales principales, y por ende un dominio de factorización única. Ahora falta solo relacionar las factorizaciones en $K[X]$ con factorizaciones en $A[X]$. Para esto nos servirá la siguiente extensión de las valuaciones p-ádicas al anillo de polinomios $K[X]$.

5.2.1. Definición (Valuaciones de Gauss). Sean A un dominio de factorización única, K su cuerpo de fracciones y $p \in A$ un elemento primo. Para un polinomio $f = \sum_{i\geq 0} a_i X^i \in K[X]$ definamos

$$v_p(f) := \min_i \{v_p(a_i)\}.$$

En particular,

$$v_p(0) = \infty.$$

De la definición debe estar claro que

$$v_p(f+g) \geq \min\{v_p(f), v_p(g)\}.$$

También tenemos la propiedad deseada para los productos.

5.2.2. Lema. *Para cualesquiera $f, g \in K[X]$ se cumple*

$$v_p(fg) = v_p(f) + v_p(g).$$

Demostración. Esto es evidente si $f = 0$ o $g = 0$, así que podemos asumir que $f, g \neq 0$. Tenemos

$$f = \sum_{i\geq 0} a_i X^i, \quad g = \sum_{j\geq 0} b_j X^j, \quad fg = \sum_{k\geq 0} c_k X^k, \quad c_k = \sum_{i+j=k} a_i b_j.$$

Ahora

$$v_p(c_k) \geq \min_{i+j=k} \{v_p(a_i) + v_p(b_j)\} \geq v_p(f) + v_p(g),$$

y por ende

$$v_p(fg) \geq v_p(f) + v_p(g).$$

Para concluir que se tiene la igualdad, hay que ver que algún coeficiente c_k tiene valuación $v_p(f) + v_p(g)$. Asumamos que $v_p(f) = v_p(a_m)$, donde el índice m es el mínimo posible:

$$v_p(a_m) < v_p(a_i) \text{ para } 0 \leq i < m, \quad v_p(a_m) \leq v_p(a_i) \text{ para } i \geq m.$$

De la misma manera, supongamos que $v_p(g) = v_p(b_n)$, donde n es el mínimo posible:

$$v_p(b_n) < v_p(b_i), \text{ para } 0 \leq i < n, \quad v_p(b_n) \leq v_p(b_i), \text{ para } i \geq n.$$

Luego,

$$v_p(c_{m+n}) \geq \min_{i+j=m+n} \{v_p(a_i) + v_p(b_j)\}.$$

Dado que $i + j = m + n$, se tiene $i < m$ o $j < n$, salvo el caso $i = m$, $j = n$. Por nuestra elección de m y n, esto significa que $v_p(a_m) + v_p(b_n)$ es estrictamente menor que otros términos, así que se puede concluir que

$$v_p(c_{m+n}) = \min_{i+j=m+n} \{v_p(a_i) + v_p(b_j)\} = v_p(a_m) + v_p(b_n) = v_p(f) + v_p(g). \qquad \blacksquare$$

5.2.3. Definición. Sean A un dominio de factorización única y K su cuerpo de fracciones. Para un polinomio $f \in K[X]$ su **contenido** está definido por

$$\operatorname{cont}(f) := \prod_p p^{v_p(f)},$$

donde el producto se toma sobre todos los primos en A salvo la relación de equivalencia $\sim$. Esto define a $\operatorname{cont}(f)$ salvo un factor invertible $u \in A^\times$, y todas las identidades con $\operatorname{cont}(f)$ serán consideradas salvo un factor invertible $u \in A^\times$.

5.2.4. Ejemplo. Consideremos los polinomios

$$f := 2X^4 + X^3 + 3X^2 + X + 1, \quad g := 3X^2 + \frac{3}{2}X + \frac{3}{2}, \quad h := \frac{2}{3}X^2 + \frac{2}{3} \in \mathbb{Q}[X].$$

Tenemos

$$\operatorname{cont}(f) = 1, \ \operatorname{cont}(g) = \frac{3}{2}, \ \operatorname{cont}(h) = \frac{2}{3}.$$

Notamos que $f = gh$ y $\operatorname{cont}(f) = \operatorname{cont}(g)\operatorname{cont}(h)$. Además,

$$\frac{g}{\operatorname{cont}(g)} = 2X^2 + X + 1, \ \frac{h}{\operatorname{cont}(h)} = X^2 + 1 \in \mathbb{Z}[X].$$

Todo esto no es una coincidencia. ▲

5.2.5. Lema. *El contenido tiene las siguientes propiedades.*

1) *Para un polinomio constante $c \in K$ se tiene* $\operatorname{cont}(c) = c$.
2) *Se tiene $f \in A[X]$ si y solamente si* $\operatorname{cont}(f) \in A$.
3) $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$ *para cualesquiera* $f, g \in K[X]$.
4) *Para $f \in K[X]$ se tiene* $\operatorname{cont}\left(\frac{1}{\operatorname{cont}(f)} f\right) = 1$, *y en particular* $\frac{1}{\operatorname{cont}(f)} f \in A[X]$.

Demostración. La parte 1) se sigue de la fórmula

$$\prod_p p^{v_p(c)} = c, \text{ salvo un factor } u \in A^\times.$$

En la parte 2), escribamos

$$f = \sum_{i \geq 0} a_i X^i \in K[X].$$

Ahora si $f \in A[X]$, entonces $v_p(a_i) \geq 0$ para todo i y todo primo $p \in A$, y luego $\operatorname{cont}(f) \in A$. Viceversa, si $\operatorname{cont}(f) \in A$, entonces $v_p(f) \geq 0$ para todo primo $p \in A$, lo que implica que $v_p(a_i) \geq 0$ para todo coeficiente a_i, y por lo tanto $a_i \in A$.

La parte 3) se sigue inmediatamente de 5.2.2, y en la parte 4) basta calcular que

$$\operatorname{cont}\left(\frac{1}{\operatorname{cont}(f)} f\right) = \operatorname{cont}\left(\frac{1}{\operatorname{cont}(f)}\right) \cdot \operatorname{cont}(f) = \frac{1}{\operatorname{cont}(f)} \cdot \operatorname{cont}(f) = 1. \qquad \blacksquare$$

5.2.6. Lema de Gauss. *Sean A un dominio de factorización única y K su cuerpo de fracciones. Entonces, los polinomios irreducibles en $A[X]$ son los siguientes:*

1) *las constantes $p \in A$ irreducibles (primas) en A;*

2) *los polionmios no constantes $f \in A[X]$ tales que* $\operatorname{cont}(f) = 1$ y *f es irreducible en $K[X]$.*

Demostración. Primero, notamos que si $p \in A$ es un polinomio constante, entonces la relación $a \mid p$ en $A[X]$ implica que $a \in A$ es también constante. De aquí se ve que las constantes irreducibles en $A[X]$ son las mismas constantes irreducibles en A.

Ahora sea $f \in A[X]$ un polinomio irreducible no constante en $A[X]$. Notamos que se tiene necesariamente $\operatorname{cont}(f) = 1$: en el caso contrario, $v_p(f) > 0$ para algún primo $p \in A$, y luego p divide a todos los coeficientes de f y por ende $p \mid f$ en $A[X]$, lo que contradice la irreducibilidad de f. Para ver que f es irreducible en $K[X]$, asumamos que en $K[X]$ se cumple

$$f = g\,h \text{ para algunos } g, h \in K[X].$$

Luego,

$$\operatorname{cont}(gh) = \operatorname{cont}(g)\operatorname{cont}(h) = \operatorname{cont}(f) = 1,$$

así que

$$f = \frac{g}{\operatorname{cont}(g)} \cdot \frac{h}{\operatorname{cont}(h)},$$

donde $\frac{g}{\operatorname{cont}(g)}$ y $\frac{h}{\operatorname{cont}(h)}$ están en $A[X]$. Por la irreducibilidad de f en $A[X]$, podemos concluir que $f \sim \frac{g}{\operatorname{cont}(g)}$ o $f \sim \frac{h}{\operatorname{cont}(h)}$ en $A[X]$, lo que implica que $f \sim g$ o $f \sim h$ en $K[X]$.

Viceversa, supongamos que para un polinomio no constante $f \in A[X]$ se tiene $\operatorname{cont}(f) = 1$ y f es irreducible en $K[X]$. Supongamos que

$$f = g\,h \text{ para algunos } g, h \in A[X].$$

Esto implica que

$$\operatorname{cont}(g)\operatorname{cont}(h) = \operatorname{cont}(f) = 1 \text{ en } A,$$

de donde $\operatorname{cont}(g) = \operatorname{cont}(h) = 1$. Luego, por la irreducibilidad de f en $K[X]$, se tiene $f \sim g$ o $f \sim h$ en $K[X]$. Asumamos por ejemplo que $f \sim g$ en $K[X]$. Esto significa que existe una constante $c \in K[X]^\times = K^\times$ tal que $f = c\,g$. Luego,

$$\operatorname{cont}(c) = \operatorname{cont}(c)\operatorname{cont}(g) = \operatorname{cont}(f) = 1,$$

y por lo tanto $c \in A^\times$ y $f \sim g$ en $A[X]$. ■

5.2.7. Ejemplo. La condición $\operatorname{cont}(f) = 1$ es necesaria. Por ejemplo, el polinomio $f := 2X^2 + 2X - 2$ es irreducible en $\mathbb{Q}[X]$ (las raíces de f son números irracionales $(-1 \pm \sqrt{5})/2$), pero f tiene una factorización no trivial $2(X^2 + X - 1)$ en $\mathbb{Z}[X]$. El número 2 es invertible en $\mathbb{Q}$, pero es primo en $\mathbb{Z}$. ▲

5.2.8. Ejemplo. La factorización en $\mathbb{Q}[X]$

$$2X^4 + X^3 + 3X^2 + X + 1 = \left(3X^2 + \frac{3}{2}X + \frac{3}{2}\right)\left(\frac{2}{3}X^2 + \frac{2}{3}\right),$$

nos da una factorización en $\mathbb{Z}[X]$

$$2X^4 + X^3 + 3X^2 + X + 1 = \frac{3}{2}(2X^2 + X + 1)\frac{2}{3}(X^2 + 1) = (2X^2 + X + 1)(X^2 + 1).$$ ▲

Estamos listos para probar la factorización única en $A[X]$.

5.2.9. Teorema. *Si A es un dominio de factorización única, entonces el anillo de polinomios $A[X]$ es también un dominio de factorización única.*

Demostración. Ya hemos verificado en 5.1.1 que toda cadena de ideales principales en $A[X]$ se estabiliza. Falta probar que todo polinomio irreducible $f \in A[X]$ es primo.

Primero, si $f \in A$ es constante, entonces f es irreducible en A, y luego es primo en A. Ahora si $f \mid ab$ para algunos $a, b \in A[X]$, entonces necesariamente $a, b \in A$, y luego $f \mid a$ o $f \mid b$. Esto demuestra que f es primo en $A[X]$.

Supongamos ahora que $\deg f > 0$. En este caso, como vimos en el lema de Gauss, $\operatorname{cont}(f) = 1$ y f es irreducible en $K[X]$. Pero $K[X]$ es un dominio de ideales principales, y en particular un dominio de factorización única, así que f es primo en $K[X]$. Asumamos que $f \mid gh$ en $A[X]$. Esto implica que $f \mid g$ o $f \mid h$ en $K[X]$. Asumamos por ejemplo que $f \mid g$. En este caso $g = f f_1$ para algún $f_1 \in K[X]$. Luego, $\operatorname{cont}(f_1) = \operatorname{cont}(f) \operatorname{cont}(f_1) = \operatorname{cont}(g) \in A$, así que $f_1 \in A$ y $f \mid g$ en $A[X]$. ■

5.2.10. Ejemplo. Se sigue que el anillo de polinomios $\mathbb{Z}[X]$ es un dominio de factorización única. Los elementos irreducibles (primos) en $\mathbb{Z}[X]$ son los primos $p = \pm 2, \pm 3, \pm 5, \pm 7, \pm 1, \ldots$ y los polinomios $f \in \mathbb{Z}[X]$ con $\operatorname{cont}(f) = 1$ que son irreducibles en $\mathbb{Q}[X]$, por ejemplo

$$f = 2X + 1, \quad 3X^2 + 2X + 2, \quad 2X^3 + 1.$$ ▲

5.2.11. Corolario. *Si A es un dominio de factorización única, entonces el anillo de polinomios en n variables $A[X_1, \ldots, X_n]$ es también un dominio de factorización única.*

Demostración. Inducción sobre n, usando isomorfismos $A[X_1, \ldots, X_n] \cong A[X_1, \ldots, X_{n-1}][X_n]$. ■

Ahora ya que sabemos que para un dominio de factorización única A los polinomios $A[X]$ también forman un dominio de factorización única, sería interesante saber cuándo un polinomio $f \in A[X]$ es irreducible. Esto es un problema profundo desde el punto de vista teórico y algorítmico, así que vamos a ver solo un par de criterios útiles en práctica: el criterio de reducción y el criterio de Eisenstein.

5.3 Criterio de reducción

5.3.1. Lema. *Sean A un anillo conmutativo e $\mathfrak{a} \subseteq A$ un ideal. Entonces, hay un isomorfismo natural*

$$A[X]/\mathfrak{a}[X] \cong (A/\mathfrak{a})[X],$$

donde $\mathfrak{a}[X]$ denota el ideal generado por $\mathfrak{a}$ en el anillo de polinomios $A[X]$:

$$\mathfrak{a}[X] := \Big\{ \sum_{i \geq 0} a_i X^i \;\Big|\; a_i \in \mathfrak{a} \Big\}.$$

Demostración. Consideremos la aplicación

$$A[X] \to (A/\mathfrak{a})[X], \quad \sum_{i \geq 0} a_i X^i \mapsto \sum_{i \geq 0} \overline{a_i} X^i$$

que reduce los coeficientes de un polinomio módulo $\mathfrak{a}$. Las fórmulas para la suma y producto de polinomios demuestran que esto es un homomorfismo de anillos. Es visiblemente sobreyectivo, y su núcleo es precisamente $\mathfrak{a}[X]$. ■

5.3.2. Proposición. *Sea A un dominio y sea $f \in A[X]$ un polinomio mónico no constante. Sea $\mathfrak{a} \subset A[X]$ un ideal propio tal que la imagen $\overline{f}$ en el cociente $A[X]/\mathfrak{a}[X] \cong (A/\mathfrak{a})[X]$ no se factoriza como un producto de polinomios de grado $< \deg \overline{f}$. Entonces, f es irreducible en $A[X]$.*

Demostración. Asumamos que f es reducible en $A[X]$; es decir,

$$f = gh, \quad g = a_m X^m + a_{m-1} X^{m-1} + \cdots, \; h = b_n X^n + b_{n-1} X^{n-1} + \cdots,$$

donde $f, g \notin A[X]^\times = A^\times$ y $a_m \neq 0$, $b_n \neq 0$. El coeficiente mayor de gh es $a_m b_n = 1$. Esto implica que $a_m, b_n \in A^\times$, y en particular g y h no son polinomios constantes, y luego $\deg g, \deg h < \deg f$. Además, en el anillo cociente $A/\mathfrak{a}$ se cumple $\overline{a_m}\,\overline{b_n} = \overline{1}$, y gracias a nuestra hipótesis de que $\mathfrak{a} \neq A$, tenemos $\overline{a_m}, \overline{b_n} \neq 0$, así que

$$\deg \overline{g} = \deg g, \quad \deg \overline{h} = \deg h.$$

La reducción módulo $\mathfrak{a}$ nos da entonces una factorización $\overline{f} = \overline{g}\,\overline{h}$, donde $\deg \overline{g}, \deg \overline{h} < \deg \overline{f}$. ■

A continuación nos va a interesar principalmente el siguiente caso particular del último resultado.

5.3.3. Corolario. *Para un polinomio mónico $f = \sum_{i\geq 0} a_i X^i \in \mathbb{Z}[X]$ y un primo p, consideremos el polinomio*

$$\overline{f} := \sum_{i\geq 0} \overline{a_i} X^i \in \mathbb{F}_p[X] \cong \mathbb{Z}[X]/(p).$$

Si $\overline{f}$ es irreducible en $\mathbb{F}_p[X]$, entonces f es irreducible en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$.

Demostración. Esta es la proposición anterior para $A = \mathbb{Z}$, $\mathfrak{a} = (p)$. La irreducibilidad en $\mathbb{Z}[X]$ implica irreducibilidad en $\mathbb{Q}[X]$ gracias al lema de Gauss. ■

5.3.4. Ejemplo. Es fácil saber cuándo un polinomio con coeficientes en $\mathbb{F}_p$ es irreducible: hay un número finito de polinomios de grado fijo. Para compilar una lista de polinomios irreducibles en $\mathbb{F}_p[X]$ se puede usar la **criba de Eratóstenes**. Por ejemplo, sea $p = 2$. Los polinomios de grado 1 son siempre irreducibles:

$$X, \quad X + 1.$$

Los polinomios de grado 2 son

$$X^2, \quad X^2 + 1, \quad X^2 + X, \quad X^2 + X + 1.$$

Entre ellos los polinomios reducibles son los productos de polinomios lineales:

$$X^2 = X \cdot X, \quad X^2 + X = X(X+1), \quad X^2 + 1 = (X+1)^2.$$

Entonces, $X^2 + X + 1$ es irreducible. Luego, los polinomios cúbicos reducibles son los productos de polinomios de grado 1 y 2:

$$\begin{aligned} X^3 &= X^3, \\ X^3 + X^2 + X + 1 &= (X+1)^3, \\ X^3 + X^2 &= X^2(X+1), \\ X^3 + X &= X(X+1)^2, \\ X^3 + X^2 + X &= (X^2 + X + 1)\,X, \\ X^3 + 1 &= (X^2 + X + 1)(X+1). \end{aligned}$$

Los dos polinomios cúbicos que nos quedan son irreducibles:

$$X^3 + X + 1, \quad X^3 + X^2 + 1.$$

Continuando de la misma manera, se puede ver que los polinomios irreducibles de grado cuatro son

$$X^4 + X + 1, \quad X^4 + X^3 + 1, \quad X^4 + X^3 + X^2 + X + 1.$$

El número de polinomios irreducibles en $\mathbb{F}_p[X]$ de grado n crece rápido con p y n. Existen métodos eficaces de factorización de polinomios en $\mathbb{F}_p[X]$: el **algoritmo de Berlekamp** y el **algoritmo de Cantor–Zassenhaus**. El lector interesado puede consultar [Coh1993, §3.4]. ▲

5.3.5. Digresión. Para los siguientes ejemplos sería útil revisar las **leyes de reciprocidad cuadrática**. Recordemos que el **símbolo de Legendre** se define para un entero a y primo p mediante

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & p \nmid a \text{ y } a \text{ es un cuadrado módulo } p, \\ -1, & p \nmid a \text{ y } a \text{ no es un cuadrado módulo } p, \\ 0, & p \mid a. \end{cases}$$

Las **leyes suplementarias** dicen para p impar se cumple

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4. \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & p \equiv 1,7 \pmod 8, \\ -1, & p \equiv 3,5 \pmod 8. \end{cases}$$

La **ley principal** nos dice que si p y q son diferentes primos impares, entonces

$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right) = \begin{cases} +\left(\frac{p}{q}\right), & \text{si } p \equiv 1 \text{ o } q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right), & \text{si } p \equiv 3 \text{ y } q \equiv 3 \pmod 4. \end{cases}$$

Para más detalles y pruebas, véanse por ejemplo mis apuntes

http://cadadr.org/san-salvador/2018-cp-tne/reciprocidad-cuadratica.pdf

5.3.6. Ejemplo. Al reducir módulo 2 el tercer polinomio ciclotómico $\Phi_3 = X^2 + X + 1 \in \mathbb{Z}[X]$ nos queda el polinomio cuadrático $\overline{\Phi_3} = X^2 + X + 1 \in \mathbb{F}_2[X]$ que no tiene raíces en $\mathbb{F}_2$ y por ende es irreducible. Podemos concluir que Φ_3 es irreducible en $\mathbb{Z}[X]$. El lema de Gauss implica que es también irreducible en $\mathbb{Q}[X]$. Notamos que si $p \neq 2$, entonces las raíces de $X^2 + X + 1$ vienen dadas por $\frac{-1 \pm \sqrt{-3}}{2}$, así que $X^2 + X + 1$ será irreducible en $\mathbb{F}_p[X]$ si y solo si -3 no es un cuadrado módulo p. Para $p \neq 2, 3$, la ley reciprocidad cuadrática nos da

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = \begin{cases} +1, & p \equiv 1 \pmod 3, \\ -1, & p \equiv 2 \pmod 3. \end{cases}$$

Para $p = 3$ tenemos $X^2 + X + 1 = (X - 1)^2$. Entonces, $X^2 + X + 1$ es irreducible en $\mathbb{F}_p[X]$ si y solamente si $p \equiv 2 \pmod 3$.

Notamos que para $\Phi_6 = \Phi_3(-X) = X^2 - X + 1$, el polinomio correspondiente $\overline{\Phi_6} \in \mathbb{F}_p[X]$ será irreducible si y solo si $\overline{\Phi_3}$ es irreducible. ▲

5.3.7. Ejemplo. Para el cuarto polinomio ciclotómico $\Phi_4 = X^2 + 1 \in \mathbb{Z}[X]$, el polinomio correspondiente $\overline{\Phi_4} = X^2 + 1$ es irreducible en $\mathbb{F}_p[X]$ si y solo si -1 no es un cuadrado módulo p. Esto sucede precisamente cuando $p \equiv 3 \pmod 4$. Podemos por ejemplo tomar $p = 3$ y concluir que Φ_4 es irreducible en $\mathbb{Z}[X]$. ▲

Los últimos ejemplos no son tan interesantes porque los polinomios en cuestión son cuadráticos, y un polinomio ciclotómico Φ_n *por la definición* no tiene raíces racionales (sus raíces son los números complejos ζ_n^k, donde $\zeta_n := e^{2\pi i/n}$ y $\operatorname{mcd}(k, n) = 1$). Podemos analizar algún polinomio ciclotómico de grado > 3.

5.3.8. Ejemplo. Consideremos el polinomio ciclotómico

$$\Phi_5 = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Z}[X].$$

Al reducirlo módulo 2, se obtiene el polinomio

$$\overline{\Phi_5} = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$$

que es irreducible. En efecto, primero se puede notar que este polinomio no tiene raíces en $\mathbb{F}_2$, así que si $\overline{\Phi_5}$ fuera reducible en $\mathbb{F}_2[X]$, este sería el producto de dos polinomios mónicos irreducibles de grado 2. Pero en $\mathbb{F}_2[X]$ hay un solo polinomio mónico irreducible de grado 2: este es X^2+X+1, y luego

$$(X^2+X+1)^2 = X^4+X^2+1.$$

Esto nos permite concluir que Φ_5 es irreducible en $\mathbb{Z}[X]$, y luego es irreducible en $\mathbb{Q}[X]$. Notamos que esto también demuestra la irreducibilidad de

$$\Phi_{10}(X) = \Phi_5(-X) = X^4 - X^3 + X^2 - X + 1. \qquad \blacktriangle$$

5.3.9. Ejemplo. El polinomio ciclotómico

$$\Phi_7 = X^6+X^5+X^4+X^3+X^2+X+1 \in \mathbb{Z}[X]$$

se vuelve reducible módulo 2: se tiene

$$\overline{\Phi_7} = (X^3+X+1)\,(X^3+X^2+1) \in \mathbb{F}_2[X].$$

Módulo 3 el polinomio sí es irreducible, pero es algo tedioso verificarlo directamente. $\blacktriangle$

Aunque nuestro criterio de irreducibilidad es muy sencillo, existen polinomios irreducibles $f \in \mathbb{Z}[X]$ tales que $\overline{f} \in \mathbb{F}_p[X]$ es reducible para cualquier primo p.

5.3.10. Ejemplo. Más adelante veremos que cualquier polinomio ciclotómico Φ_n es irreducible en $\mathbb{Z}[X]$ (y luego en $\mathbb{Q}[X]$). Sin embargo, resulta que $\Phi_8 = X^4+1$ se vuelve reducible módulo cualquier primo. Por ejemplo, tenemos las siguientes factorizaciones.

$$\begin{aligned}
p=2:&\quad (X+1)^4,\\
p=3:&\quad (X^2+X+2)\,(X^2+2X+2),\\
p=5:&\quad (X^2+2)\,(X^2+3),\\
p=7:&\quad (X^2+3X+1)\,(X^2+4X+1),\\
p=11:&\quad (X^2+3X+10)\,(X^2+8X+10),\\
p=13:&\quad (X^2+5)\,(X^2+8),\\
p=17:&\quad (X+2)\,(X+8)\,(X+9)\,(X+15),\\
&\quad \cdots
\end{aligned}$$

En efecto, para $p=2$ se tiene la factorización $X^4+1=(X+1)^4$. Para p impar tenemos necesariamente $p \equiv 1,3,5,7 \pmod 8$.

- Si $p \equiv 1 \pmod 8$, entonces $p \equiv 1 \pmod 4$, y en este caso -1 es un cuadrado módulo p. Tenemos $-1=a^2$ para algún $a \in \mathbb{F}_p$ y podemos escribir

$$X^4+1 = X^4-a^2 = (X^2+a)\,(X^2-a).$$

- Si $p \equiv 3 \pmod 8$, entonces $p \equiv 3 \pmod 4$ y ni -1, ni 2 no es un cuadrado módulo p. En este caso -2 es un cuadrado. Si $-2=a^2$, entonces

$$(X^2+aX-1)\,(X^2-aX-1) = X^4-(2+a^2)\,X+1 = X^4+1.$$

- Si $p \equiv 5 \pmod 8$, entonces $p \equiv 1 \pmod 4$, y el polinomio se reduce como en el caso de $p \equiv 1 \pmod 8$ de arriba.

- Si $p \equiv 7 \pmod 8$, entonces 2 es un cuadrado módulo p; se tiene $2=a^2$ para algún $a \in \mathbb{F}_p$, y luego

$$(X^2+aX+1)\,(X^2-aX+1) = X^4+(2-a^2)\,X+1 = X^4+1.$$

De hecho, en el caso $p \equiv 1 \pmod 8$ el polinomio X^4+1 se factoriza como *cuatro* diferentes polinomios lineales en $\mathbb{F}_p[X]$: a saber, si $\alpha \in \mathbb{F}_p^\times$ es un generador de $\mathbb{F}_p[X]$ y $\beta := \alpha^{\frac{p-1}{8}}$, entonces

$$X^4+1 = (X-\beta)(X-\beta^3)(X-\beta^5)(X-\beta^7).$$

Una raíz de X^4+1 en $\mathbb{F}_p$ siempre corresponde a un elemento de orden 8 en $\mathbb{F}_p^\times$, así que para $p \equiv 3,5,7 \pmod 8$ el polinomio no puede tener raíces y se factoriza en dos polinomios cuadráticos irreducibles como indicado arriba.

Entonces, para $\frac{3}{4}$ de los primos p el polinomio X^4+1 se factoriza en $\mathbb{F}_p[X]$ como un producto de dos polinomios cuadráticos irreducibles, y para $\frac{1}{4}$ de los primos la factorización es un producto de cuatro diferentes polinomios lineales. El primo $p=2$ es excepcional en este sentido.

En general, los patrones de factorización de un polinomio irreducible $f \in \mathbb{Z}[X]$ módulo diferentes primos p se explica en la teoría de números algebraica por el famoso **teorema de Frobenius** y **teorema de densidad de Chebotarëv**[*]. Para más detalles, véase [LS1996]. ▲

5.4 Criterio de Eisenstein

Otro criterio de irreducibilidad útil en práctica es el criterio de Eisenstein. Antes de formularlo, consideremos un ejemplo particular.

5.4.1. Ejemplo. Consideremos el polinomio mónico

$$X^4+4X^3+6X^2+4X+2 \in \mathbb{Z}[X].$$

Asumamos que este es reducible y

$$X^4+4X^3+6X^2+4X+2 = fg,$$

donde $f,g \in \mathbb{Z}[X]$ y $f,g \notin \mathbb{Z}[X]^\times$. Todos los coeficientes de nuestro polinomio son divisibles por 2, así que reduciendo la identidad de arriba módulo 2, se obtiene

$$X^4 = \overline{f}\,\overline{g} \text{ en } \mathbb{F}_2[X],$$

donde $\overline{f}$ y $\overline{g}$ son los polinomios f y g con coeficientes reducidos módulo 2. Ahora $\mathbb{F}_2[X]$ es un dominio de factorización única, donde X^4 se factoriza como $X^2 \cdot X^2$ o $X \cdot X^3$, así que $\overline{f}$ y $\overline{g}$ tienen esta forma, y en particular $2 \mid f(0)$ y $2 \mid g(0)$. Pero esto implicaría que $4 \mid fg(0)$, mientras que $fg(0) = 2$. Podemos entonces concluir que nuestro polinomio es irreducible en $\mathbb{Z}[X]$. ▲

El último ejemplo funciona porque todos los coeficientes del polinomio son divisibles por 2 y el coeficiente constante no es divisible por 4. Esto se generaliza de la siguiente manera.

5.4.2. Teorema (Criterio de Eisenstein). *Sean A un dominio y $p \in A$ un elemento primo. Sea*

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

un polinomio mónico con coeficientes en A tales que $p \mid a_i$ para todo $i = 0,1,\ldots,n-1$, pero $p^2 \nmid a_0$. Entonces, f es irreducible.

Demostración. Asumamos que f es reducible y $f = gh$ donde $g,h \notin A[X]^\times = A^\times$. Notamos que necesariamente

$$1 \le \deg g, \deg h < n$$

—si uno de estos polinomios fuera constante, este sería invertible, dado que f es un polinomio mónico. Reduciendo módulo p, se obtiene una identidad

$$\overline{X^n} = \overline{f} = \overline{g}\,\overline{h} \quad \text{en } A/(p)[X]$$

[*] Nikolaĭ Chebotarëv (1894–1947), matemático soviético.

por la hipótesis sobre los coeficientes de f. Puesto que p es primo, el cociente $A/(p)$ es un dominio, y podemos encajarlo en su cuerpo de fracciones $K := \operatorname{Frac} A/(p)$. La identidad de arriba considerada en $K[X]$ implica que

$$\overline{g} = c\,X^k, \quad \overline{h} = c^{-1}\,X^\ell,$$

para algún $c \in K^\times$ y $k + \ell = n$. Notamos que $k \le \deg g$ y $\ell \le \deg h$, así que $k, \ell < n$, lo que implica que $k, \ell > 0$.

Sin embargo, si ambos g y h se reducen a un polinomio sin término constante, esto significa que los términos constantes de g y h son divisibles por p. Esto implicaría que el término constante de f es divisible por p^2 que no es el caso por nuestra hipótesis. ■

5.4.3. Ejemplo. Probemos que el polinomio $f = X^2 + Y^2 - Z^2$ es irreducible en el anillo $\mathbb{C}[X, Y, Z]$.

Usando la identificación $\mathbb{C}[X, Y, Z] \cong \mathbb{C}[Y, Z][X]$, podemos considerar f como un polinomio en X con término constante $Y^2 - Z^2$. Notamos que $Y^2 - Z^2$ es reducible en $\mathbb{C}[Y, Z]$: se tiene

$$Y^2 - Z^2 = (Y + Z)\,(Y - Z).$$

El polinomio lineal $p := Y + Z$ es irreducible, y tenemos $p \mid (Y^2 - Z^2)$, pero $p^2 \nmid (Y^2 - Z^2)$. Entonces, el criterio de Eisenstein implica que f es irreducible. Podemos generalizar este argumento al caso de

$$f = X^n + Y^n - Z^n \in \mathbb{C}[X, Y, Z].$$

Notamos que $Y^n - Z^n$ se factoriza en distintos polinomios lineales $\mathbb{C}[Y, Z]$:

$$Y^n - Z^n = \prod_{0 \le k \le n-1} (Y - \zeta_n^k Z).$$

En particular, para el polinomio $p := Y - Z$ se tiene $p \mid (Y^n - Z^n)$, pero $p^2 \nmid (Y^n - Z^n)$.

Las ecuaciones de la forma $X^n + Y^n - Z^n$ se conocen como las **ecuaciones de Fermat**. El **último teorema de Fermat** (demostrado en 1995 por el matemático inglés Andrew Wiles con ayuda de Richard Taylor) afirma que para $n > 2$ sus únicas soluciones racionales son de la forma

$$\begin{cases} \{(x, 0, x), (0, y, y)\}, & n \text{ impar}, \\ \{(\pm x, 0, \pm x), (0, \pm y, \pm y)\}, & n \text{ par}. \end{cases}$$

▲

5.5 Irreducibilidad de Φ_{p^k}

Una aplicación típica del criterio de Eisenstein es la irreducibilidad de los polinomios ciclotómicos

$$\Phi_{p^k} = X^{p^{k-1}(p-1)} + X^{p^{k-1}(p-2)} + \cdots + X^{p^{k-1}} + 1 \in \mathbb{Z}[X].$$

Aquí el término constante es igual a 1, así que el criterio de Eisenstein no se aplica directamente. Para este motivo vamos a sustituir $X + 1$ en lugar de X. Por ejemplo,

$$\Phi_8(X + 1) = (X + 1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2,$$

y el criterio de Eisenstein sí funciona para $p = 2$.

5.5.1. Lema. *Para todo $a \in A$ un polinomio no constante $f \in A[X]$ es irreducible si y solo si $f(X+a)$ es irreducible.*

Demostración. Notamos que $\deg f(X) = \deg f(X + a)$. Una factorización no trivial $f(X + a) = g(X)\,h(X)$ nos daría una factorización $f(X) = g(X - a)\,h(X - a)$. ■

5.5.2. Proposición. *Para todo primo p el polinomio Φ_p es irreducible en $\mathbb{Z}[X]$ (y entonces en $\mathbb{Q}[X]$).*

Demostración. El polinomio $\Phi_p(X)$ es irreducible si y solo si $\Phi_p(X+1)$ es irreducible. Notamos que

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1)-1} = \frac{1}{X}\sum_{1\le k\le p}\binom{p}{k}X^k$$
$$= \binom{p}{p}X^{p-1} + \binom{p}{p-1}X^{p-2} + \cdots + \binom{p}{3}X^2 + \binom{p}{2}X + \binom{p}{1}.$$

Los coeficientes de arriba satisfacen

$$p \mid \binom{p}{k} \text{ para todo } 1 \le k < p \quad \text{y} \quad p^2 \nmid \binom{p}{1} = p.$$

Entonces, se puede aplicar el criterio de Eisenstein para el primo p. ■

5.5.3. Proposición. *Para todo primo p y $k \ge 1$ el polinomio Φ_{p^k} es irreducible en $\mathbb{Z}[X]$ (y entonces en $\mathbb{Q}[X]$).*

Demostración. Ya vimos el caso de $k = 1$. Podemos asumir entonces que $k \ge 2$. De nuevo, consideremos la sustitución

$$\Phi_{p^k}(X+1) = \frac{(X+1)^{p^k}-1}{(X+1)^{p^{k-1}}-1} = \sum_{0\le i\le p-1}(X+1)^{i\,p^{k-1}}.$$

Tenemos para todo $k \ge 2$

$$(X+1)^{p^{k-1}} \equiv X^{p^{k-1}} + 1 \pmod{p},$$

y luego

$$\Phi_{p^k}(X+1) \equiv \sum_{0\le i\le p-1}(X^{p^{k-1}}+1)^i = \frac{(X^{p^{k-1}}+1)^p - 1}{(X^{p^{k-1}}+1)-1}$$
$$= \frac{(X^{p^{k-1}}+1)^p - 1}{X^{p^{k-1}}} \equiv \frac{X^{p^k}}{X^{p^{k-1}}} = X^{p^{k-1}(p-1)} \pmod{p}.$$

Esto significa que todos los coeficientes menores de $\Phi_{p^k}(X+1)$ son divisibles por p. El coeficiente constante es igual a

$$\Phi_{p^k}(1) = \Phi_p(1^{p^{k-1}}) = \Phi_p(1) = p,$$

y de nuevo podemos aplicar el criterio de Eisenstein. ■

5.6 Irreducibilidad de Φ_n (♣)

En realidad, *cualquier* polinomio ciclotómico Φ_n es irreducible en $\mathbb{Z}[X]$, no solamente cuando $n = p^k$. Esto fue probado por Gauss y no es tan fácil. Primero formulemos algunos lemas.

5.6.1. Lema. *Sea ζ cualquier raíz n-ésima primitiva de la unidad. Entonces, todas las raíces n-ésimas primitivas son de la forma ζ^k para* $\mathrm{mcd}(k,n) = 1$.

Demostración. Las raíces n-ésimas primitivas son precisamente ζ_n^k, donde $\zeta_n = e^{2\pi i/n}$ y $\mathrm{mcd}(k,n) = 1$. Ahora supongamos que $\zeta = \zeta_n^k$. Tenemos $1 = an + bk$ para algunos $a, b \in \mathbb{Z}$. Tenemos $\mathrm{mcd}(b,n) = 1$. Notamos que

$$\zeta^b = \zeta_n^{1-an} = \zeta_n\,(\zeta_n^n)^{-a} = \zeta_n.$$

■

5.6.2. Ejemplo. Las raíces octavas primitivas son

$$\zeta_8,\ \zeta_8^3,\ \zeta_8^5,\ \zeta_8^7.$$

Podemos escribirlas como

$$\zeta_8 = (\zeta_8^3)^3, \quad \zeta_8^3, \quad \zeta_8^5 = (\zeta_8^3)^7, \quad \zeta_8^7 = (\zeta_8^3)^5. \qquad \blacktriangle$$

5.6.3. Lema (Polinomio mínimo). *Sean $\alpha \in \mathbb{C}$ un número complejo y $f \in \mathbb{Z}[X]$ un polinomio mónico irreducible tal que $f(\alpha) = 0$. Si $g \in \mathbb{Z}[X]$ es otro polinomio mónico tal que $g(\alpha) = 0$, entonces $f \mid g$.*

Demostración. La irreducibilidad de f en $\mathbb{Z}[X]$ implica su irreducibilidad en $\mathbb{Q}[X]$. Notamos que f y g pertenecen al núcleo del homomorfismo de evaluación

$$\phi\colon \mathbb{Q}[X] \to \mathbb{C}, \quad h \mapsto h(\alpha).$$

Pero $\mathbb{Q}[X]$ es un dominio de factorización única, así que $\ker\phi = (h)$ para algún polinomio no constante $h \in \mathbb{Q}[X]$. Tenemos entonces $h \mid f$ y $h \mid g$. La irreducibilidad de f implica que $h \sim f$, y luego $f \mid g$ en $\mathbb{Q}[X]$. Dado que f y g son mónicos, se sigue que $f \mid g$ en $\mathbb{Z}[X]$. ■

Normalmente los polinomios ciclotómicos Φ_n se vuelven reducibles en $\mathbb{F}_p[X]$, como en el caso de Φ_8 que se vuelve reducible módulo cualquier primo p. Sin embargo, nuestro argumento ocupará de alguna manera ingeniosa las factorizaciones de $\overline{\Phi_n}$ en $\mathbb{F}_p[X]$.

5.6.4. Lema. *Para cualquier polinomio $g \in \mathbb{F}_p[X]$ se cumple $g(X^p) = g^p$.*

Demostración. Usando la fórmula del binomio en característica p y el pequeño teorema de Fermat $a^p = a$ para todo $a \in \mathbb{F}_p$, tenemos

$$(a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0)^p = a_n (X^p)^n + a_{n-1} (X^p)^{n-1} + \cdots + a_1 X^p + a_0. \qquad \blacksquare$$

5.6.5. Ejemplo. $(X^2 + X + 1)^2 = X^4 + 2X^3 + 3X^2 + 2X + 1 \equiv X^4 + X^2 + 1 \pmod 2$. ▲

5.6.6. Lema. *Si $p \nmid n$, entonces en la factorización del polinomio ciclotómico Φ_n en $\mathbb{F}_p[X]$ no hay factores repetidos.*

Demostración. Gracias a la fórmula

$$X^n - 1 = \prod_{d \mid n} \Phi_n,$$

sería suficiente probar que en la factorización de $X^n - 1$ en $\mathbb{F}_p[X]$ no hay factores repetidos. Supongamos que en $\mathbb{F}_p[X]$

$$X^n - 1 = f^2 g$$

para algunos polinomios no constantes $f, g \in \mathbb{F}_p[X]$. Luego, tomando las derivadas se obtiene

$$n X^{n-1} = 2 f f' g + f^2 g' = f (2 f' g + f g').$$

Entonces, $f \mid (X^n - 1)$ y $f \mid n X^{n-1}$. Sin embargo, si $p \nmid n$, entonces $\operatorname{mcd}(X^n - 1, n X^{n-1}) = 1$. Esto se sigue por ejemplo, de la identidad de Bézout

$$\frac{X}{n} \cdot (n X^{n-1}) - (X^n - 1) = 1. \qquad \blacksquare$$

5.6.7. Ejemplo. Volvamos al ejemplo 5.3.10. El polinomio ciclotómico $\Phi_8 = X^4 + 1$ se factoriza en $\mathbb{F}_2[X]$ como $(X + 1)^4$. Luego, si $p \equiv 1 \pmod 8$, entonces $X^4 + 1$ es un producto de cuatro diferentes polinomios lineales, y si $p \equiv 3, 5, 7 \pmod 8$, entonces $X^4 + 1$ es un producto de dos diferentes polinomios cuadráticos irreducibles. Los factores repetidos salen solo para $p = 2$. ▲

5.6.8. Teorema (Gauss). *Para cualquier $n = 1, 2, 3, \ldots$ el polinomio ciclotómico Φ_n es irreducible en $\mathbb{Z}[X]$ (y entonces en $\mathbb{Q}[X]$).*

Demostración. Escribamos

$$\Phi_n = fg$$

para algunos polinomios $f, g \in \mathbb{Z}[X]$, donde f es irreducible. Dado que Φ_n es mónico, el coeficiente mayor de f y g es ± 1, y podemos asumir que son también mónicos. Sea ζ una raíz n-ésima primitiva. Tenemos entonces

$$\Phi_n(\zeta) = f(\zeta)\, g(\zeta) = 0.$$

Esto implica que $f(\zeta) = 0$ o $g(\zeta) = 0$. Puesto que f no es constante, alguna raíz n-ésima primitiva ζ debe ser una raíz de f, y nuestro objetivo es probar que todas las raíces primitivas

$$\zeta^k, \quad \operatorname{mcd}(k, n) = 1$$

son raíces de f.

Asumamos entonces que $f(\zeta) = 0$ y sea p un número primo tal que $p \nmid n$. Entonces, ζ^p es también una raíz n-ésima primitiva y

$$\Phi_n(\zeta^p) = f(\zeta^p)\, g(\zeta^p) = 0.$$

Asumamos que $g(\zeta^p) = 0$. Luego, el lema 5.6.3 implica que $f \mid g(X^p)$ en $\mathbb{Z}[X]$. Reduciendo módulo p y aplicando el lema 5.6.4, se obtiene $\overline{f} \mid \overline{g}^p$ en $\mathbb{F}_p[X]$. Pero esto implica que $\overline{\Phi_n} = \overline{f}\,\overline{g}$ tiene un factor repetido en su factorización en $\mathbb{F}_p[X]$, lo que contradice el lema 5.6.6. Entonces, $f(\zeta^p) = 0$.

Esto demuestra que para cualquier primo p tal que $p \nmid n$ se tiene

$$f(\zeta) = 0 \Longrightarrow f(\zeta^p) = 0.$$

Ahora todas las raíces n-ésimas primitivas son de la forma ζ^k donde $\operatorname{mcd}(n, k) = 1$. Podemos factorizar entonces $k = p_1 \cdots p_s$ donde p_i son primos (no necesariamente diferentes) tales que $p_i \nmid n$, y luego

$$\zeta^k = (((\zeta^{p_1})^{p_2})^{\cdots})^{p_s}.$$

El argumento de arriba nos dice que $f(\zeta^{p_1}) = 0$. Luego, el mismo argumento aplicado a ζ^{p_1} demuestra que $f((\zeta^{p_1})^{p_2}) = 0$, etcétera, y en fin $f(\zeta^k) = 0$. Entonces, todas las raíces n-ésimas primitivas son raíces de f y por ende $g = 1$. ∎

5.6.9. Digresión. La idea principal del argumento de arriba es probar que *si para un polinomio* $f \in \mathbb{Z}[X]$ *se tiene* $f(\zeta) = 0$ *para una raíz* n*-ésima primitiva* ζ*, entonces* $f(\zeta^k) = 0$ *para todo* k *tal que* $\operatorname{mcd}(k, n) = 1$.

He aquí otro modo de establecerlo. Primero notamos que para cualquier primo p se tiene $f(\zeta^p) \equiv f(\zeta)^p \pmod{p}$ en el anillo $\mathbb{Z}[\zeta_n]$. En efecto, $\mathbb{Z}[\zeta_n]/(p)$ es un anillo de característica p, y luego

$$f(\zeta^p) = x^{mp} + a_{m-1}x^{(m-1)p} + \cdots + a_1 x^p + a_0 \equiv (x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0)^p = f(\zeta)^p \pmod{p}.$$

Ahora, el **teorema de Dirichlet sobre primos en progresiones aritméticas** (!) afirma que para todo k tal que $\operatorname{mcd}(k, n) = 1$ hay un número infinito de primos p que cumplen $p \equiv k \pmod{n}$. Entonces,

$$p \mid f(\zeta^p) = f(\zeta^k) \quad \text{en } \mathbb{Z}[\zeta_n]$$

para un número infinito de p, lo que implica que $f(\zeta^k) = 0$.

Sin embargo, no es tan fácil demostrar el teorema de Dirichlet: la prueba se basa en la teoría de números analítica. El lector interesado puede consultar [IR1990, Chapter 16].

5.6.10. Comentario. El 12 de junio de 1808 Gauss anotó en su diario matemático que había probado la irreducibilidad de Φ_n para cualquier n. Sin embargo, su argumento original se considera perdido. La primera demostración publicada pertenece a Kronecker (1854).

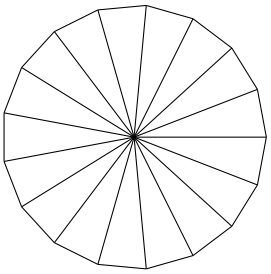
Gauss hizo un estudio extensivo de las raíces de la unidad y polinomios ciclotómicos en su tratado "Disquisitiones Arithmeticae" publicado en 1801 [Gau1801]. Como una aplicación curiosa de la teoría, él encontró una expresión algebraica para la raíz de la unidad

$$\zeta_{17} = \cos\left(\frac{2\pi}{17}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{17}\right).$$

A saber,

$$\cos\left(\frac{2\pi}{17}\right) = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34-2\sqrt{17}} + \frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

(y luego $\mathrm{sen}(2\pi/17)$ se encuentra como $\sqrt{1-\cos^2(2\pi/17)}$). Puesto que las raíces cuadradas pueden ser construidas con regla y compás, esto demuestra la posibilidad de construir con regla y compás el **heptadecágono** (el polígono regular de 17 lados).



Gauss estaba tan orgulloso de su descubrimiento que quería grabar el heptadecágono en su lápida, pero el artesano encargado se negó, dado que esta figura no se distinguiría del círculo.

5.7 Ejercicios

Ejercicio 5.1. Demuestre que para todo $n = 1, 2, 3, \ldots$ el polinomio $(X-1)(X-2)\cdots(X-n)-1$ es irreducible en $\mathbb{Z}[X]$.

Ejercicio 5.2. El contenido puede ser definido de otra manera más transparente. Como siempre, denotemos por A un dominio de factorización única y por K el cuerpo de fracciones de A.

a) Demuestre que para $f = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$ se tiene $\operatorname{cont}(f) = \operatorname{mcd}(a_0, a_1, \ldots, a_n)$.

b) Demuestre que todo polinomio $f \in K[X]$ puede ser escrito como $\frac{1}{d} g$, donde $d \in A$ y $g \in A[X]$, y luego $\operatorname{cont}(f) = \frac{\operatorname{cont}(g)}{d}$.

Ejercicio 5.3. Sean A un dominio de factorización única, y $f, g \in A[X]$. Demuestre que

$$\operatorname{cont}(\operatorname{mcd}(f,g)) = \operatorname{mcd}(\operatorname{cont}(f), \operatorname{cont}(g)).$$

Ejercicio 5.4. Sean k un cuerpo, $f \in k[X_1, \ldots, X_n]$ un polinomio en n variables y $f = f_1^{m_1} \cdots f_s^{m_s}$ una factorización de f, donde $f_1, \ldots, f_s$ son polinomios irreducibles no asociados entre sí y $m_1, \ldots, m_s \geq 1$. Demuestre que para cualquier otro polinomio $g \in k[X_1, \ldots, X_n]$ las siguientes condiciones son equivalentes:

a) $f^r \mid g$ para algún $r = 1, 2, 3, \ldots$;

b) $f_1 \cdots f_s \mid g$.

Sugerencia: use el hecho de que $k[X_1, \ldots, X_n]$ es un dominio de factorización única y factorice f^r y g en polinomios irreducibles.

Ejercicio 5.5 (Teorema de las raíces racionales). Sea

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

un polinomio con coeficientes enteros. Demuestre que si $\frac{a}{b}$ es una raíz racional de f tal que $\operatorname{mcd}(a,b) = 1$, entonces $a \mid a_0$ y $b \mid a_n$.
Sugerencia: extraiga el factor lineal $(bX - a)$ de f.

Ejercicio 5.6. Sea c un entero no nulo.

a) Demuestre que el polinomio $X^3 + nX + c$ es irreducible en $\mathbb{Q}[X]$ para todo $n \in \mathbb{Z}$, salvo un número finito de excepciones.

b) En particular, para $c = 2$ encuentre las factorizaciones del polinomio $f = X^3 + nX + 2$ para todo n.

Sugerencia: use el ejercicio anterior.

Ejercicio 5.7. Demuestre que el polinomio $f := X^3 + 2X + 1$ es irreducible en $\mathbb{Q}[X]$ usando

a) el lema de Gauss y la reducción módulo algún primo p;

b) el teorema de las raíces racionales.

Ejercicio 5.8. Consideremos el polinomio $f = X^3 + 8X^2 + 6 \in \mathbb{Z}[X]$.

a) Demuestre que f es irreducible en $\mathbb{Q}[X]$ usando el criterio de Eisenstein.

b) Demuestre que f es irreducible en $\mathbb{Q}[X]$ usando el teorema de las raíces racionales.

c) Factorice $\overline{f}$ en $\mathbb{F}_p[X]$ para $p = 2, 3, 5, 7$.

(En efecto, el primer primo p tal que $\overline{f}$ queda irreducible en $\mathbb{F}_p[X]$ es 29.)

Ejercicio 5.9. Encuentre un polinomio cúbico irreducible $f \in \mathbb{Q}[X]$ que tiene tres raíces reales.

Ejercicio 5.10. Demuestre que el polinomio $X^n - p$ es irreducible en $\mathbb{Q}[X]$ para todo primo $p = 2, 3, 5, 7, \ldots$ y todo $n = 1, 2, 3, \ldots$

Ejercicio 5.11. Factorice el polinomio $X^n + Y^n$ en polinomios lineales en $\mathbb{C}[X, Y]$.

Ejercicio 5.12. Para un número primo p, factorice el polinomio ciclotómico Φ_{p^k} en $\mathbb{F}_p[X]$.

Ejercicio 5.13. Demuestre que el polinomio $Y^n - X^3 + X$ es irreducible en el anillo $k[X, Y]$, donde $n = 1, 2, 3, \ldots$ y k es cualquier cuerpo.

Ejercicio 5.14. Consideremos el polinomio

$$f := X^4 - 10\,X^2 + 1 \in \mathbb{Q}[X].$$

a) Demuestre que f no tiene factores lineales en $\mathbb{Q}[X]$.

b) Demuestre que f no se factoriza en dos polinomios cuadráticos en $\mathbb{Z}[X]$.

c) Deduzca de b) que f tampoco se factoriza en dos polinomios quadráticos en $\mathbb{Q}[X]$.
(Sugerencia: use el contenido.)

d) Deduzca de a), b), c) que f es irreducible en $\mathbb{Q}[X]$.

Bibliografía

[Coh1993] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag Berlin Heidelberg, 1993.
https://doi.org/10.1007/978-3-662-02945-9

[Gau1801] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, 1801, Versión española (Hugo Barrantes, Michael Josephy, Angel Ruiz). Centro de Investigaciones Matemáticas y Meta-Matemáticas, Universidad de Costa Rica, 2008.
http://cimm.ucr.ac.cr/da/

[IR1990] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716
https://doi.org/10.1007/978-1-4757-2103-4

[LS1996] Hendrik Willem Lenstra and Peter Stevenhagen, *Chebotarëv and his density theorem*, The Mathematical Intelligencer (1996), no. 18, 26–37. MR1395088
http://www.math.leidenuniv.nl/~hwl/papers/cheb.pdf