Def: El n-esimo polinomio ciclotomico, denotado $\Phi_n(x)$, es el polinomio mónico en $\mathbb{C}[x]$ cuyas raices son las raices n-esimas primitivas de la unidad.

Tenemos que

$$\Phi_n(x) = \prod_{\substack{\xi \\ n\text{-esima raiz} \\ \text{primitiva}}} (x-\xi) = \prod_{\substack{mcd(k,n)=1 \\ k<n}} \left(x - e^{\frac{2\pi i k}{n}}\right)$$

Por lo tanto $gr(\Phi_n(n)) = \varphi(n)$

$\Phi_1(x) = X-1$, $\Phi_2(x) = X-(-1) = X+1$

$\Phi_3(x) = (x-\omega)(x-\omega^2)$ donde $\omega = e^{\frac{2\pi i}{3}}$ $\omega^2 = \bar{\omega}$

$= -\frac{1}{2} + \frac{\sqrt{3}}{2} i$

Lema: $x^n - 1 = \prod_{d|n} \Phi_d(x)$

Note que comparando los grados de los polinomios en la igualdad de arriba obtenemos $n = \sum_{d|n} \varphi(d)$.

Dem:

Las raices de $x^n - 1$ en $\mathbb{C}$ son todas las raices n-esimas de la unidad en $\mathbb{C}$ y así $x^n - 1 = \prod (x - \xi)$ donde ξ corre sobre todas las raices n-esimas de la unidad.

Cada raiz n-esima de la unidad tiene orden d donde d es un divisor de n. Asi cada raiz n-esima de la unidad es una raiz d-esima primitiva para un divisor d de n.

Reciprocamente, cada raiz d-esima

primitiva de la unidad con d un divisor de n, es una raiz n-esima de la unidad

Agrupando

$$X^n - 1 = \prod_{d \mid n} \prod (x - \zeta)$$

donde ζ corre sobre las raices d-esimas primitivas de la unidad.

Cor. Todos los coeficientes de Φ_n están en $\mathbb{Z}$.

Dem:

Primero demostraremos que $\Phi_n \in \mathbb{Q}[x]$. Sea $E=\mathbb{Q}[\xi]$ con ξ un raiz n-esima primitiva de la unidad. Por lo tanto E es el campo de descomposicion de Φ_n. Notemos que Φ_n es separable. Así $E \supseteq \mathbb{Q}$ es de Galois. Consideremos ξ una raiz n-esima primitiva de la unidad y $\sigma \in Gal(E/\mathbb{Q})$. Entonces $\sigma(\xi)$ es también una raiz n-esima primitiva de la unidad. Así $\sigma(\Phi_n) = \Phi_n$ para cada $\sigma \in Gal(E/\mathbb{Q})$

Por lo tanto los coeficientes de Φ_n estan en $Fix(Gal(E/\mathbb{Q})) = \mathbb{Q}$.

Ahora, $\Phi_n(x)$ divide a $x^n - 1$ en $\mathbb{Q}[x]$.

es decir, $x^n - 1 = \Phi_n(x) g(x)$ con $g(x) \in \mathbb{Q}[x]$

Como $\Phi_n(x)$ es mónico entonces

$\Phi_n(x) \in \mathbb{Z}[x]$..

Teorema: Φ_n es irreducible para cada n. en $\mathbb{Z}[x]$.

Dem:

Supongamos que $\Phi_n(x)$ no es irreducible y consideremos un factor monico irreducible $f(x)$ de $\Phi_n(x)$ que tiene a una raiz n-esima primitiva de la unidad ξ como raiz.

Entonces $f(x)$ no tiene a cada raiz n-esima de la unidad como raíz, así que existe $k>1$ tal que $f(\xi^k)\neq 0$. Tomemos el mínimo de estos k y consideramos un factor primo p de k. Como k es primo relativo a n, entonces p y k/p también lo son. Sea $\omega=\xi^{k/p}$. Por la minimalidad de k, $f(\omega)=0$ pero $f(\omega^p)\neq 0$

El polinomio irreducible $f(x)$ es tambien un factor de x^n-1, es decir, $x^n-1=f(x)g(x)$ con $f(x), g(x) \in \mathbb{Z}[x]$. Entonces

$$0=(\omega^p)^n-1=f(\omega^p)g(\omega^p)$$

Por lo tanto $g(\omega^p)=0$. Escribamos $g(x)=\sum a_i x^i$ con $a_i \in \mathbb{Z}$. Entonces

$$0=g(\omega^p)=\sum a_i(\omega^p)^i=\sum a_i \omega^{pi}.$$ Así

$h(\omega)=0$ con $h(x)=g(x^p)\in \mathbb{Z}[x]$

Como $f(\omega)=0$ y $f(x)$ es monico irreducible, $f(x)$ divide a $h(x)$ en $\mathbb{Q}[x]$. y entonces lo divide en $\mathbb{Z}[x]$.

Consideremos el morfismo $\pi: \mathbb{Z}[x] \to \frac{\mathbb{Z}}{p\mathbb{Z}}[x]$ la reducción modulo p. Entonces $\pi(f(x))$ divide a $\pi(h(x))$ en $\frac{\mathbb{Z}}{p\mathbb{Z}}[x]$. Note que

$$\pi(h(x)) = \pi(g(x^p)) = \left(\pi(g(x))\right)^p$$

Así $\pi(f(x)) \mid (\pi(g(x)))^p$ en $\mathbb{Z}/p\mathbb{Z}[x]$.

y por lo tanto $\pi(f(x))$ y $\pi(g(x))$ comparten un factor irreducible $\overline{q}(x)$.

Pero $x^n - 1 = \pi(x^n - 1) = \pi(f(x))\pi(g(x))$

lo que implica que $\overline{q}(x)^2 \mid x^n - 1$ en $\mathbb{Z}/p\mathbb{Z}[x]$.

Esto implica que $x^n - 1$ tiene un factor lineal repetido en un campo de descomposición

Sobre $\mathbb{Z}/p\mathbb{Z}$. Sin embargo x^n-1 tiene todas sus raíces distintas ∇

Por lo tanto, $\Phi_n(x)$ es irreducible.

Ejemplos

$$x^n-1=\prod_{d\mid n}\Phi_d(x) \Rightarrow \Phi_n(x)=\frac{x^n-1}{\prod_{\substack{d\mid n\\ d<n}}\Phi_d(x)}$$

Para un primo p

$$\Phi_p(x)=\frac{x^p-1}{\Phi_1(x)}=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\dots+x+1$$

$$\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\,\Phi_2(x)} = \frac{x^4-1}{(x-1)(x+1)} = \frac{x^4-1}{x^2-1}$$

$$= x^2+1.$$

$$\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)} = \frac{x^6-1}{(x^2-1)(x^2+x+1)}$$

$$= x^2-x+1.$$

$\vdots$

Denotemos ξ_n el numero complejo $e^{\frac{2\pi i}{n}}$, así ξ_n es una raiz n-esima primitiva de la unidad. Escribimos $\mathbb{Q}_n = \mathbb{Q}[\xi_n]$ y lo llamamos el n-ésimo campo ciclotómico. Para $n>0$ denotamos U_n al grupo de unidades de $\mathbb{Z}/n\mathbb{Z}$.

Lema: Sea C es un grupo ciclico de orden n. Entonces $Aut(C) \cong U_n$, en particular $Aut(C)$ es abeliano. Si n es primo, $Aut(C)$ es ciclico de orden $n-1$.

Lema: Sea $F \subseteq E$ y supongamos que $E = F[\xi]$ donde ξ es una raiz m-esima de la unidad. Entonces E es Galois sobre F y $Gal(E/F)$ es isomorfo a un subgrupo de $Aut(C)$ donde $C = \langle \xi \rangle \leq E^*$. En particular $Gal(E/F)$ es abeliano.

Dem:

Sea n el orden multiplicativo de ξ, entonces ξ es una raiz n-esima primitiva de

de la unidad y E es el campo de descomposicion de x^n-1 sobre F. Como E contiene n raices n-esimas de la unidad x^n-1 tiene n raices en E. Por lo tanto x^n-1 es separable. Asi $E \supseteq F$ es de Galois.

Si $\sigma \in Gal(E/F)$, $\sigma(\xi)$ es una raiz n-esima de la unidad y así $\sigma(\xi) \in C = \langle \xi \rangle$. Por lo tanto $\sigma(C) = C$. Así σ define un automorfismo de C y entonces tenemos un morfismo de grupos $Gal(E/F) \to Aut(C)$ dado por la restriccion. Como $E = F[\xi]$

si $\sigma(\xi) = \xi$, entonces σ fija a $F(\xi) = E$

Por lo tanto $\sigma = e$. Así tenemos un

morfismo inyectivo $Gal(E/F) \longrightarrow Aut(C)$.

Cor. $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$.

Dem:

$\mathbb{Q}_n = \mathbb{Q}(\xi_n)$ ent $[\mathbb{Q}_n : \mathbb{Q}] = gr(\min_{\mathbb{Q}}(\xi_n))$

$\min_{\mathbb{Q}}(\xi_n) = \Phi_n(x)$ $\therefore [\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$

Cor. $Gal(\mathbb{Q}_n/\mathbb{Q}) \cong Aut(C) \cong U_n$ donde C es un grupo ciclico de orden n.

Dem:

$\varphi(n) = [\mathbb{Q}_n : \mathbb{Q}] = |Gal(\mathbb{Q}_n/\mathbb{Q})| \leq |Aut(C)|$

$= |U_n| = \varphi(n)$

$\therefore Gal(\mathbb{Q}_n/\mathbb{Q}) \cong Aut(C) \cong U_n$.

Teorema: Sea $l = mcm(m,n)$ y $d = mcd(m,n)$. Entonces:

a) $\langle \mathbb{Q}_m, \mathbb{Q}_n \rangle = \mathbb{Q}_l$ donde $\langle \mathbb{Q}_m, \mathbb{Q}_n \rangle$ es el menor campo en $\mathbb{C}$ que contiene a $\mathbb{Q}_m$ y a $\mathbb{Q}_n$.

b) $\mathbb{Q}_m \cap \mathbb{Q}_n = \mathbb{Q}_d$.