ÁLGEBRA III (Doble grado Informática-Matemáticas)

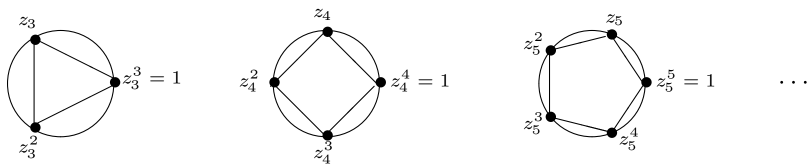
4. Extensiones Ciclotómicas, Radicales y Cíclicas

4.1. **Extensiones ciclotómicas.**

Recordar que, si $a \in \mathbb{C}$ es cualquier complejo no nulo, para cualquier natural $n \geq 2$, las raíces complejas del polinomio $x^n - a$, esto es, los números complejos z tales que $z^n = a$, son llamadas las **raíces n-ésimas del número** a (cuadradas si $n = 2$, cúbicas si $n = 3$, etc.). Un caso particular de especial interés, son las **raíces n-ésimas de la unidad**, esto es las raíces del polinomio $x^n - 1$. Para cada entero $n \geq 1$, estas conforman un subgrupo de orden n del grupo multiplicativo de los complejos

$$\mathbb{C}_n = \{z \in \mathbb{C}^\times \mid z^n = 1\} \leq \mathbb{C}^\times$$

En efecto, si $z, z' \in \mathbb{C}_n$, entonces $(zz')^n = z^n z'^n = 1 \cdot 1 = 1$. Además $(z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1$. Así que $\mathbb{C}_n$ es cerrado para productos, inversos, y contiene al 1. Es por tanto un grupo. Podemos ser más explícitos en la descripción de las raíces n-ésimas de la unidad: Con la representación geométrica de los números complejos como puntos del plano $\mathbb{R}^2$ en mente, si dividimos el círculo de radio 1 en n sectores circulares de igual amplitud, esto es, todos de amplitud $\frac{2\pi}{n}$, y ubicamos el primero de ellos sobre el eje positivo de abscisas se nos determinan los n vértices de un polígono regular de n lados inscrito en la circunferencia $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$,



que corresponderían justo a los n números complejos $e^{\frac{2k\pi i}{n}} = \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}$, para $k = 1, \ldots, n$. Todos estos listan las n raíces n-ésimas de la unidad, pues $(e^{\frac{2k\pi i}{n}})^n = e^{2k\pi i} = \cos 2k\pi + i \sin 2k\pi = 1$, así que

$$\mathbb{C}_n = \{e^{\frac{2k\pi i}{n}},\ 1 \leq k \leq n\}.$$

Entre esas n diferentes raíces complejas de la unidad hay una especial, que es llamada la **raíz n-ésima primitiva de la unidad**:

$$z_n = e^{\frac{2\pi i}{n}} = cos\frac{2\pi}{n} + i\, sen\frac{2\pi}{n},$$

que tiene la propiedad de ser un generador del grupo $\mathbb{C}_n$, ya que $z_n^k = e^{\frac{2k\pi i}{n}}$ y, por tanto, $\mathbb{C}_n = \{1, z_n, z_n^2, \ldots, z_n^{n-1}\} = \langle z_n \mid z_n^n = 1\rangle$ *es un grupo cíclico de orden n generado por* z_n.

Definición 1. *Si $K \leq \mathbb{C}$ es cualquier cuerpo de números, para cada entero $n \geq 1$, el cuerpo extensión $K(z_n)$ es llamado el n-ésimo* **cuerpo ciclotómico sobre** K*, o la n-ésima* **extension ciclotómica de** K*. Particularmente nos referimos a $\mathbb{Q}(z_n)$ como al n-ésimo* **cuerpo ciclotómico**.

Los siguientes son los primeros ejemplos de extensiones ciclotómicas,

- $z_1 = 1$, así que $K(z_1) = K$.
- $z_2 = -1$, luego $K(z_2) = K$.
- $z_3 = \omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, por tanto $K(z_3) = K(\omega) = K(i\sqrt{3})$.
- $z_4 = i$, luego $K(z_4) = K(i)$.

Notemos que $K(z_n) = K(x^n - 1)$, el cuerpo de descomposición del polinomio $x^n - 1$ sobre K. Por tanto la extensión ciclotómica $K(z_n)/K$ **es una extensión de normal**, cuyo grado será el grado del polinomio $Irr(z_n, K)$ que, al ser un divisor de $x^n - 1$, siempre ser $\leq n$. Intentamos a continuación conocer más información sobre el polinomio $Irr(z_n, K)$ y el grupo de Galois $G(K(z_n)/K) = G(x^n - 1/K)$.

Sabemos que, en el grupo $\mathbb{C}_n$, $or(z_n^k) = \frac{n}{(k,n)}$. En particular, $or(z_n^k) = n$, esto es, z_n^k es un generador de $\mathbb{C}_n$, si y solo si $(k, n) = 1$. Entonces,

$$Gen(\mathbb{C}_n) = \{z \in \mathbb{C}_n \mid or(z) = n\} = \{z_n^k \mid 1 \leq k \leq n,\ mcd(k, n) = 1\}$$

y $\mathbb{C}_n$ tiene exactamente $\varphi(n)$ generadores, donde φ es la función de Euler. Recordar que, si $p_1, \ldots, p_r$ son los diferentes primos positivos que dividen al natural n, digamos que $n = p_1^{e_1} \cdots p_r^{e_r}$, entonces

$$\begin{aligned}
\varphi(n) &= p_1^{e_1-1}(p_1 - 1) \cdots p_r^{e_r-1}(p_r - 1) = p_1^{e_1-1} p_1 \Big(1 - \frac{1}{p_1}\Big) \cdots p_r^{e_r-1} p_r \Big(1 - \frac{1}{p_r}\Big) \\
&= p_1^{e_1}\Big(1 - \frac{1}{p_1}\Big) \cdots p_r^{e_1}\Big(1 - \frac{1}{p_r}\Big) = p_1^{e_1} \cdots p_r^{e_r}\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_r}\Big) \\
&= n\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_r}\Big).
\end{aligned}$$

Definición 2. *Se define el n-***ésimo polinomio ciclotómico** Φ_n *por la fórmula*

$$\Phi_n = \prod_{z \in Gen(\mathbb{C}_n)} (x - z) = \prod_{\substack{1 \leq k \leq n \\ (k,n) = 1}} (x - z_n^k)\,.$$

Esto es, Φ_n es el polinomio mónico de grado $\varphi(n)$ cuya raíces son las raíces n-ésimas de la unidad de orden n. Los siguientes son unos primeros ejemplos

- $Gen(\mathbb{C}_1) = \{1\}$, y $\Phi_1 = x - 1$.
- $Gen(\mathbb{C}_2) = \{-1\}$, y $\Phi_2 = x + 1$.
- $Gen(\mathbb{C}_3) = \{\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \omega^2 = \overline{\omega}\}$, por tanto
$$\Phi_3 = (x - \omega)(x - \overline{\omega}) = x^2 - (\omega + \overline{\omega})x + \omega\overline{\omega} = x^2 + x + 1\,.$$
- $Gen(\mathbb{C}_4) = \{i, i^3 = -i\}$, y $\Phi_4 = (x - i)(x + i) = x^2 + 1$.

El siguiente hecho es muy útil para el cálculo recursivo de los polinomios ciclotómicos.

Proposición 3. *Para todo natural $n \geq 1$ se verifica que*

$$x^n - 1 = \prod_{d|n} \Phi_d\,.$$

Demostración. Trabajando en el grupo multiplicativo $\mathbb{C}^\times$, tenemos que

$$\begin{aligned}
\mathbb{C}_n = \{z \in \mathbb{C}^\times \mid z^n = 1\} = \{z \in \mathbb{C}^\times \mid or(z)|n\} &= \bigcup_{d|n} \{z \in \mathbb{C}^\times \mid or(z) = d\} \\
&= \bigcup_{d|n} Gen(\mathbb{C}_d)\,,
\end{aligned}$$

siendo esa unión disjunta. Entonces,

$$x^n - 1 = \prod_{z \in \mathbb{C}_n} (x - z) = \prod_{\substack{d|n \\ z \in Gen(\mathbb{C}_d)}} (x - z) = \prod_{d|n} \prod_{z \in Gen(\mathbb{C}_d)} (x - z) = \prod_{d|n} \Phi_d\,.$$

$\square$

Los siguientes ejemplos ilustran el uso de la anterior relación para cálculos:

- $x - 1 = \Phi_1$.
- $x^2 - 1 = \Phi_1\Phi_2$, de donde $\Phi_2 = x + 1$.
- $x^3 - 1 = \Phi_1\Phi_3$, de donde $\Phi_3 = \frac{x^3-1}{x-1} = x^2 + x + 1$.
- Si p es un primo, $x^p - 1 = \Phi_1\Phi_p$, de donde

$$\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

- $x^6 - 1 = \Phi_1\Phi_2\Phi_3\Phi_6 = (\Phi_1\Phi_3)\Phi_2\Phi_6 = (x^3 - 1)(x + 1)\Phi_6$, de donde

$$\Phi_6 = \frac{x^6 - 1}{(x^3 - 1)(x + 1)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1.$$

El siguiente teorema muestra que los polinomios ciclotómicos tienen sus coeficientes números enteros, y entonces $\Phi_n \in K[x]$ para todo cuerpo de números K, de manera que $Irr(z_n, K)|\Phi_n$ en $K[x]$. Para su demostración usaremos el siguiente lema:

Lema 4. *1) Sea $g \in \mathbb{Q}[x]$ mónico, entonces $g = \frac{1}{a}g_1$ donde $a \geq 1$ y $g_1 \in \mathbb{Z}[x]$ es primitivo. 2) Sea $f \in \mathbb{Z}[x]$ mónico. Si $f = gh$ con $g, h \in \mathbb{Q}[x]$ mónicos, entonces $g, h \in \mathbb{Z}[x]$.*

Demostración. 1) Supongamos $g = \dfrac{a_0}{b_0} + \cdots + \dfrac{a_{n-1}}{b_{n-1}}x^{n-1} + x^n$. Sea $b = mcd(b_i)$. Claramente entonces $c_i = \dfrac{ba_i}{b_i} \in \mathbb{Z}$ para todo $i = 0, \ldots, n-1$, y $bg = c_0 + \cdots + c_{n-1}x^{n-1} + bx^n \in \mathbb{Z}[x]$. Siendo $c = mcd(c_0, \ldots, c_{n-1}, b)$ su contenido, será $bg = cg_1$ con $g_1 \in \mathbb{Z}[x]$ primitivo. Puesto que $c|b$, será $b = ac$ para un cierto $a \geq 1$. Pero entonces

$$g = \frac{1}{b}bg = \frac{1}{b}cg_1 = \frac{1}{ac}cg_1 = \frac{1}{a}g_1.$$

2) Pongamos $g = \dfrac{1}{a}g_1$ y $h = \dfrac{1}{b}h_1$, con $a, b \geq 1$ y $g_1, h_1 \in \mathbb{Z}[x]$ primitivos. Entonces $f = \dfrac{1}{ab}g_1h_1$ y $abf = g_1h_1$. Puesto que f es primitivo (es mónico) y g_1 y h_1 también, por el Lema de Gauss (*“El contenido de un producto es el producto de los contenidos”*), concluimos que $ab = 1$ y consecuentemente que $a = b = 1$. $\square$

Teorema 5. * *Para todo $n \geq 1$, $\Phi_n \in \mathbb{Z}[x]$.*

Demostración. Probamos primero que $\Phi_n \in \mathbb{Q}[x]$. Notemos que $\mathbb{C}_n \subseteq \mathbb{Q}(z_n)$. Supongamos cualquier $\sigma \in G(\mathbb{Q}(z_n)/\mathbb{Q})$. Entonces para todo $z \in \mathbb{C}_n$ se verifica que $\sigma(z) \in \mathbb{C}_n$, pues $\sigma(z)^n = \sigma(z^n) = \sigma(1) = 1$. Se sigue que σ restringe definiendo un automorfismo del grupo $\mathbb{C}_n$, $\sigma : \mathbb{C}_n \cong \mathbb{C}_n$, y entonces también restringe a una permutación $\sigma : Gen(\mathbb{C}_n) \cong Gen(\mathbb{C}_n)$. Notemos que, por construcción, $\Phi_n \in \mathbb{Q}(z_n)[x]$. Si suponemos entonces que $\Phi_n = \sum a_i x^i$ con $a_i \in \mathbb{Q}(z_n)$, de la cadena de igualdades

$$\Phi_n^\sigma = \sum \sigma(a_i)x^i = \prod_{z \in Gen(\mathbb{C}_n)} (x - z)^\sigma = \prod_{z \in Gen(\mathbb{C}_n)} (x - \sigma(z)) = \prod_{z \in Gen(\mathbb{C}_n)} (x - z) = \Phi_n(x)\,,$$

deducimos que $\sigma(a_i) = a_i$ para todo i y todo $\sigma \in G(\mathbb{Q}(z_n)/\mathbb{Q})$. De donde todo coeficiente $a_i \in \mathbb{Q}(z_n)^{G(\mathbb{Q}(z_n)/\mathbb{Q})} = \mathbb{Q}$. Así que $\Phi_n \in \mathbb{Q}[x]$.

Finalmente, puesto que $x^n - 1 = \Phi_n \prod_{d|n, d \neq n} \Phi_d$, el lema anterior nos permite concluir que, efectivamente, $\Phi_n \in \mathbb{Z}[x]$. $\square$

Nuestro objetivo a continuación es probar que $\Phi_n = Irr(z_n, \mathbb{Q})$. Para ello, necesitamos unos resultados auxiliares. Entre ellos, el significado de los términos binomiales

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} = \frac{n(n-1)\cdots(n-i+1)}{i(i-1)\cdots 2\cdot 1}.$$

y que, en cualquier anillo conmutativo, digamos A, se verifica la fórmula binomial

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i},$$

donde el producto na de enteros $n \geq 0$ por elementos $a \in A$ es el usual: Si $n = 0$, entonces $0a = 0$; si $n > 0$, entonces $na = \sum_{i=1}^{n} a$ es la suma reiterada de ese elemento a consigo mismo n veces. En efecto, para $n = 1$ es fácil

$$\binom{1}{0} a^0 b^1 + \binom{1}{1} a^1 b^0 = b + a = a + b = (a+b)^1.$$

Y, para $n > 1$, su demostración es inductiva apoyándose en la igualdad

$$\begin{aligned}\binom{n}{j} + \binom{n}{j-1} &= \frac{n!}{j!(n-j)!} + \frac{n!}{(j-1)!(n-j+1)!} = \frac{n!(n-j)!(j-1)!(n-j+1+j)}{j!(n-j)!(j-1)!(n-j+1)!} \\ &= \frac{n!(n+1)}{j!(n-j+1)!} = \binom{n+1}{j}.\end{aligned}$$

Supuesta la validez para un n, entonces

$$\begin{aligned}(a+b)^{n+1} = (a+b)(a+b)^n &= (a+b)\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} = \sum_{i=0}^{n} \binom{n}{i} a^{i+1} b^{n-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n+1-i} \\ &= \sum_{i=1}^{n+1} \binom{n}{i-1} a^i b^{n+1-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n+1-i} \\ &= \sum_{i=1}^{n+1} \binom{n+1}{i} a^i b^{n+1-i} + b^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i}.\end{aligned}$$

Necesitamos también recordar que, para cada entero $n \geq 2$, tenemos el anillo de clases de congruencia módulo n,

$$\mathbb{Z}_n = \{[m] \mid m \in \mathbb{Z}\}$$

donde

$$\begin{aligned}[m] = [m'] &\Leftrightarrow m \equiv m' \mod n \\ &\Leftrightarrow n \mid m - m' \\ &\Leftrightarrow m - m' \in n\mathbb{Z} \\ &\Leftrightarrow m \text{ y } m' \text{ dan el mismo resto al dividirlos por } n,\end{aligned}$$

con las operaciones ordinarias de suma y producto de clases

$$[m] + [m'] = [m + m'], \ [m][m'] = [mm'].$$

Este sabemos que es efectivamente un anillo con exactamente n elementos distintos, que se listan como las clases módulo n de los n diferentes restos que se obtienen al dividir todos los enteros enteros entre n; esto es, las clases $[0], [1], \ldots, [n-1]$ que solemos denotar también simplemente por $0, 1, \ldots, n-1$. Así, es usual simplificar la notación y poner

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

con las operaciones

$$m + m' = \text{ resto de dividir en } \mathbb{Z} \text{ el entero m+m' entre } p,$$
$$mm' = \text{ resto de dividir en } \mathbb{Z} \text{ el entero producto de } mm' \text{ entre } p,$$

para cuales quiera $0 \leq m, m' \leq n - 1$.

Haremos uso del epimorfismo de anillos **reducción módulo** n,

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}_n, \qquad m \mapsto \overline{m} = \text{ resto de dividir } m \text{ entre } n,$$

y del correspondiente inducido,

$$\mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}_n[x], \qquad f = \textstyle\sum_i m_i x^i \mapsto \overline{f} = \sum_i \overline{m}_i x^i \ .$$

También haremos uso del grupo multiplicativo $\mathbb{Z}_n^\times$ de las unidades (elementos inversibles) del anillo $\mathbb{Z}_n$. Explícitamente,

$$\mathbb{Z}_n^\times = \{k \in \mathbb{Z}_n, \ mcd(k, n) = 1\} = \{k \mid 1 \leq k \leq n, \ mcd(k, n) = 1\}.$$

En efecto, supongamos que $k \in \mathbb{Z}_n$ con $mcd(k, n) = 1$. por el Teorema de Bezout, existirán $u, v \in \mathbb{Z}$ tal que $1 = uk + vn$. Pero entonces

$$1 = \overline{1} = \overline{uk} + \overline{vn} = \overline{uk} + 0 = \overline{u}\overline{k} = \overline{u}k$$

y concluimos que k es invertible en $\mathbb{Z}_n$, con $k^{-1} = \overline{u}$. Y recíprocamente, supongamos que $k \in \mathbb{Z}_n^\times$. Será $ku = 1$ (en $\mathbb{Z}_n$) para un cierto $u \in \mathbb{Z}_n$, lo que significa que 1 es el resto de dividir en $\mathbb{Z}$ el producto de los enteros k y u; esto es, si q es el correspondiente cociente, será $1 = ku - qn$. Y esta última igualdad implica que $mcd(k, n) = 1$ (pues si $d > 1$ fuese un divisor común, digamos que $k = dk'$ y $n = un'$, entonces $1 = d(k'u - qn')$ lo que en $\mathbb{Z}$ es imposible).

Para el siguiente lema auxiliar, supondremos que $p > 0$ es cualquier primo positivo de $\mathbb{Z}$. Notemos que, en este caso, $\mathbb{Z}_p^\times = \{1, \ldots, p - 1\}$ y $\mathbb{Z}_p$ es un cuerpo.

Lema 6. *Sea $\mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}_p[x]$, $f = \sum_i m_i x^i \mapsto \overline{f} = \sum_i \overline{m}_i x^i$, el epimorfismo de reducción módulo un primo p.*

(i) Para cualesquiera $f, g \in \mathbb{Z}[x]$, se verifica que

$$(\overline{f} + \overline{g})^p = \overline{f}^p + \overline{g}^p.$$

(ii) Para cualquier $m \in \mathbb{Z}$, $\overline{m}^p = \overline{m}$.

(iii) Para cualesquiera $m_1, \ldots, m_r \in \mathbb{Z}$ y $f_1, \ldots, f_r \in \mathbb{Z}[x]$, se verifica que

$$(\overline{m}_1 \overline{f}_1 + \cdots + \overline{m}_r \overline{f}_r)^p = \overline{m}_1 \overline{f}_1^p + \cdots + \overline{m}_r \overline{f}_r^p.$$

(iv) Para cualquier $g \in \mathbb{Z}[x]$, se verifica que

$$\overline{g}^p = \overline{g}(x^p),$$

donde $\overline{g}(x^p)$ es el polinomio resultante de sustituir x en $\overline{g}$ por x^p.

Demostración. (i):

$$(\overline{f} + \overline{g})^p = \overline{(f + g)^p} = \overline{\sum_{i=0}^{p} \binom{p}{i} f^i g^{p-i}} = \sum_{i=0}^{p} \overline{\binom{p}{i}} \overline{f}^i \overline{g}^{p-i} = \overline{f}^p + \overline{g}^p.$$

(ii) Este es el Pequeño Teorema de Fermat: El grupo $\mathbb{Z}_p^\times$ es de orden $p - 1$, por tanto, si $\overline{m} \neq 0$, se tendrá que $\overline{m}^{p-1} = 1$. Luego $\overline{m}^p = \overline{m}$ sea m cualquiera.

(iii) Es consecuencia de (i) y (ii), y se argumenta por una simple inducción en r.

(iv) Supongamos $g = \sum_{i=0}^{n} m_i x^i$. Entonces

$$\overline{g}^p = (\sum_i \overline{m}_i x^i)^p = (\sum_i \overline{m}_i \overline{x^i})^p = \sum_i \overline{m}_i \overline{x^{ip}} = \sum_i \overline{m}_i (x^p)^i = \overline{g}(x^p). \quad \square$$

Con todo lo anterior, podemos ya abordar el siguiente

Teorema 7. *Para todo natural $n \geq 1$ el polinomio Φ_n es irreducible en $\mathbb{Q}[x]$. Entonces,*

$$\Phi_n = Irr(z_n, \mathbb{Q}).$$

Demostración. Pongamos $f = Irr(z_n, \mathbb{Q})$. Probaremos a continuación que, para toda raíz z de f y cualquier primo p con $p \nmid n$ se tiene que z^p es también una raíz de f. Un uso reiterado de esta propiedad nos conduce a que $z_n^{p_1^{m_1} \cdots p_r^{m_r}}$ es una raíz de f para todos los primos $p_1, \ldots p_r$ que no dividan a n; esto es, a que z_n^k es una raíz de f siempre que $(k, n) = 1$. Pero esto implica que f tiene a todo elemento del conjunto $Gen(\mathbb{C}_n)$ como una de sus raíces, lo que implica que $gr(f) \geq \varphi(n)$; puesto que $f | \Phi_n$ y ambos son mónicos, concluimos que $f = \Phi_n$. Así que, $\Phi_n = Irr(z_n, \mathbb{Q})$.

Supongamos entonces que $f(z) = 0$ y que p es un primo con $p \nmid n$.

Notemos que ha de ser $x^n - 1 = fg$ para un cierto polinomio $g \in \mathbb{Q}[x]$, y el Lema 4 nos asegura que $f, g \in \mathbb{Z}[x]$. Como $z^p \in \mathbb{C}_n$, $0 = (z^p)^n - 1 = f(z^p)g(z^p)$ y, por tanto, $f(z^p) = 0$ o $g(z^p) = 0$. La demostración se reduce a ver que no es posible que $g(z^p) = 0$: Supongamos, por contrario, que $g(z^p) = 0$. Consideremos el polinomio $g(x^p)$, que tiene entonces a z como raíz. Como $f = Irr(z, \mathbb{Q})$, ha de ser $f | g(x^p)$ (necesariamente en $\mathbb{Z}[x]$, de nuevo por el Lema 4). Considerando ahora el epimorfismo de reducción módulo p, $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$, $h(x) \mapsto \overline{h}(x)$, tenemos que $\overline{f} | \overline{g}(x^p)$ en el anillo $\mathbb{Z}_p[x]$. Puesto que $\overline{g}(x^p) = \overline{g}^p$, concluimos que $\overline{f} | \overline{g}^p$ en el anillo $\mathbb{Z}_p[x]$, lo que particularmente implica que toda raíz del polinomio $\overline{f}$ (en cualquier cuerpo extensión de $\mathbb{Z}_p$) es también una raíz del polinomio $\overline{g}$. Pero, dada la igualdad $x^n - 1 = \overline{f}(x)\overline{g}(x)$ en $\mathbb{Z}_p[x]$, esto nos lleva a que el polinomio $x^n - 1 \in \mathbb{Z}_p[x]$ tiene raíces múltiples. Pero esto es contradictorio (ver Proposición 1.1 en Tema 1), ya que el derivado de este polinomio es

$$nx^{n-1} = x^{n-1} + \stackrel{n}{\cdots} + x^{n-1} = (1 + \stackrel{n}{\cdots} + 1)x^{n-1} = \overline{n}x^{n-1},$$

que es asociado de x^{n-1} (recordemos que $p \nmid n$ y por tanto $\overline{n} \neq 0$), y claramente primo relativo con $x^n - 1$. $\square$

Nos centramos ahora en el grupo de Galois de una extensión ciclotómica.

Teorema 8. * *Para cualquier cuerpo de números K, hay un monomorfismo de grupos*

$$G(K(z_n)/K) \to \mathbb{Z}_n^\times, \quad \sigma \mapsto k \text{ si } \sigma(z_n) = z_n^k.$$

En particular, $G(\mathbb{Q}(z_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$.

Demostración. Sea $\sigma \in G(K(z_n)/K)$. Puesto que z_n es raíz de Φ_n que es un polinomio de $\mathbb{Q}[x]$ (también entonces $\Phi \in K[x]$, pues $\mathbb{Q} \leq K$) y por tanto $\Phi_n^\sigma = \Phi_n$, necesariamente $\sigma(z_n)$ será otra raíz de Φ_n (ver Lema 3 en Tema 3), esto es $\sigma(z_n) = z_n^k$ para un cierto $k \in \mathbb{Z}_n^\times$. Podemos definir así la aplicación

$$f : G(K(z_n)/K) \to \mathbb{Z}_n^\times, \quad \sigma \mapsto f(\sigma) = k \text{ si } \sigma(z_n) = z_n^k.$$

Esta aplicación es inyectiva, pues cada σ está totalmente determinada por quien sea la imagen del generador $\sigma(z_n)$. Y es efectivamente un monomorfismo de grupos: Sean $\sigma, \tau \in$

$G(K(z_n)/K)$ con $f(\sigma) = k$ y $f(\tau) = j$. Supongamos que $j\,k = q\,n + r$, con $0 \leq r \leq n-1$. entonces $f(\sigma)f(\tau) = r$, y como

$$\sigma\tau(z_n) = \sigma(z_n^j) = \sigma(z_n)^j = (z_n^k)^j = z_n^{kj} = z_n^{qn+r} = (z_n^n)^q z_n^r = z_n^r\,,$$

concluimos que $f(\sigma\tau) = r = f(\sigma)f(\tau)$ en el anillo $\mathbb{Z}_n$.

En el caso particular $K = \mathbb{Q}$, el resultado se sigue dado que ambos grupos $G(\mathbb{Q}(z_n)/K)$ y $\mathbb{Z}_n^\times$ son del mismo orden, $\varphi(n)$. $\square$

Corolario 9. *Toda extensión ciclotómica tiene grupo de Galois abeliano.*

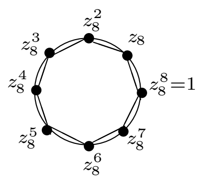
Ejemplo 10. *Sea z_8 la raíz octava primitiva de la unidad.*

(1) *Describir los complejos z_8^k, $1 \leq k \leq 8$, en la forma $a+bi$ y representarlos geométricamente como puntos en el plano Euclídeo.*
(2) *Calcular Φ_8.*
(3) *Describir el grupo $G(\mathbb{Q}(z_8)/\mathbb{Q})$ y probar que es isomorfo al grupo de Klein $K = \langle u, v \mid u^2 = 1, v^2 = 1, uv = vu\rangle$ ($\cong \mathbb{C}_2 \times \mathbb{C}_2$).*
(4) *Describir su retículo de subgrupos de $G(\mathbb{Q}(z_8)/\mathbb{Q})$.*
(5) *Describir el retículo de subcuerpos de $\mathbb{Q}(z_8)$.*

Solución: (1) Puesto que $z_8 = cos(\pi/4) + i\,sen(\pi/4)$, tenemos que

$$\begin{cases} z_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, & z_8^2 = i, \quad z_8^3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \quad z_8^4 = -1, \\ z_8^5 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, & z_8^6 = -i, \quad z_8^7 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \quad z_8^8 = 1. \end{cases}$$

Su representación geométrica en el plano consiste de los 8 vértices del octógono inscrito en la circunferencia S^1



(2) Puesto que $x^8 - 1 = \Phi_1\Phi_2\Phi_4\Phi_8$ y $\Phi_1\Phi_2\Phi_4 = x^4 - 1$, concluimos que

$$\Phi_8 = \frac{x^8-1}{x^4-1} = x^4 + 1.$$

(3) Conocemos que que el grupo de Galois $G(\mathbb{Q}(z_8)/\mathbb{Q})$ es isomorfo al grupo de las unidades del anillo de restos módulo 8, $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$. Analizando este grupo, donde $j \cdot k = \overline{j\,k}$ (= resto de dividir el producto de j y k en $\mathbb{Z}$ entre 8), vemos que es un grupo de orden 4 tipo Klein, pues es abeliano y todos sus elementos no triviales son de orden 2: $3^2 = 1$, $5^2 = 1$, $7^2 = 1$. Entonces

$$G = \{\sigma_j \mid\, :\ \sigma_j(z_8) = z_8^j,\ j = 1, 3, 5, 7\},$$

con multiplicación $\sigma_j\sigma_k = \sigma_{\overline{j\cdot k}}$. Por el Teorema de Dyck (ya que $\sigma_3^2 = id = \sigma_5^2$ y $\sigma_3\sigma_5 = \sigma_5\sigma_3$) existe un homomorfismo $\phi : K \to G$ tal que $\phi(u) = \sigma_3$ y $\phi(v) = \sigma_5$. Su imagen también contiene a $\sigma_7 = \sigma_3\sigma_5 = \phi(uv)$ y, obviamente, a $\sigma_1 = id$, y es por tanto un epimorfismo. Puesto que K y G tiene ambos cuatro elementos, $\phi : K \cong G$ es un isomorfismo.

(4) El grupo de Galois tiene entonces tres subgrupos propios, todos cíclicos de orden 2: $\langle\sigma_3\rangle$, $\langle\sigma_5\rangle$ y $\langle\sigma_7\rangle$. Y el retículo de subgrupos será de la forma

$$\begin{tikzcd}
 & G(\mathbb{Q}(z_8)/\mathbb{Q}) & \\
\langle\sigma_3\rangle \arrow[ur, "2"] & \langle\sigma_5\rangle \arrow[u, "2"] & \langle\sigma_7\rangle \arrow[ul, "2"'] \\
 & 1 \arrow[ul, "2"] \arrow[u, "2"] \arrow[ur, "2"'] &
\end{tikzcd}$$

(5) Por el Teorema Fundamental de la Teoría de Galois, existen exactamente tres cuerpos intermedios, que serán los subcuerpos fijos correspondientes a los tres subgrupos anteriores. Para determinar el subcuerpo fijo bajo σ_3, discutamos la ecuación $\sigma_3(\alpha) = \alpha$, con $\alpha = a_0 + a_1 z_8 + a_2 z_8^2 + a_3 z_8^3$, donde los $a_j \in \mathbb{Q}$. Como $\sigma_3(\alpha) = a_0 + a_1 z_8^3 + a_2 z_8^6 + a_3 z_8^9$, si tenemos en cuenta que $z_8^8 = 1$ y que $z_8^4 = -1$, resulta que $\sigma_3(\alpha) = \alpha$ si y solo si

$$a_0 + a_1 z_8^3 - a_2 z_8^2 + a_3 z_8 = a_0 + a_1 z_8 + a_2 z_8^2 + a_3 z_8^3.$$

Lo que se verifica si y solo si $a_1 = a_3$ y $a_2 = 0$. Por tanto

$$\mathbb{Q}(z_8)^{\sigma_3} = \{a + b(z + z^3),\ a, b \in \mathbb{Q}\}.$$

Ahora,como $z + z^3 = (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) + (-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = i\sqrt{2}$, concluimos que

$$\mathbb{Q}(z_8)^{\sigma_3} = \mathbb{Q}(i\sqrt{2})\,.$$

Procediendo del mismo modo, calculamos los otros dos subcuerpos fijos y concluimos el retículo de subcuerpos es

$$\begin{tikzcd}
 & \mathbb{Q} \arrow[dl, "2"'] \arrow[d, "2"] \arrow[dr, "2"] & \\
\mathbb{Q}(i\sqrt{2}) \arrow[dr, "2"] & \mathbb{Q}(i) \arrow[d, "2"] & \mathbb{Q}(\sqrt{2}) \arrow[dl, "2"'] \\
 & \mathbb{Q}(z_8) &
\end{tikzcd}$$

4.2. **Extensiones radicales y cíclicas.**

Recordemos que, si $0 \neq a = re^{i\theta} = r(cos\,\theta + i\,sen\,\theta)$ es cualquier complejo no nulo expresado en su forma polar, entonces el complejo $\sqrt[n]{r}\,e^{i\frac{\theta}{n}}$ es una particular raíz n-ésima de a a la que denotaremos por $\sqrt[n]{a}$. Esto es,

$$\sqrt[n]{a} = \sqrt[n]{r}\,e^{i\frac{\theta}{n}} = \sqrt[n]{r}\left(cos\frac{\theta}{n} + i\,sen\frac{\theta}{n}\right).$$

Y también que el conjunto de las n diferentes n raíces n-ésimas de a (es decir, raíces complejas de $x^n - a$) es

$$\{\sqrt[n]{a},\ \sqrt[n]{a}\,z_n,\ \sqrt[n]{a}\,z_n^2,\ \ldots,\ \sqrt[n]{a}\,z_n^{n-1}\},$$

donde $\sqrt[n]{a}\,z_n^k = \sqrt[n]{r}\,e^{i\frac{\theta+2k\pi}{n}}$ para cada $k = 1, \ldots, n$.

Por una **extensión radical** de un cuerpo de números $K \leq \mathbb{C}$ se entiende una extensión simple de este cuerpo, que es generada por una raíz n-ésima, para algún $n \geq 1$, de algún número $a \in K$. Dicho de otra forma, una extensión radical de K es un cuerpo de la forma

$K(\alpha)$, donde $\alpha^n = a \in K$ para algún $n \geq 1$. Alternativamente, también podemos decir que una extensión radical de un cuerpo de números K es un cuerpo de números de la forma $K(\sqrt[n]{a}z_n^k)$ para algún $a \in K$, algún $n \geq 1$ y algún k con $1 \leq k \leq n$. Por ejemplo, las extensiones ciclotómicas son extensiones radicales.

Las extensiones radicales están muy relacionadas con las llamadas **extensiones cíclicas**, esto es, extensiones normales E/K cuyo grupo de Galois $G(E/K)$ es cíclico. Para establecer esta relación, haremos uso del siguiente resultado conocido como el Lema de independencia de Dedekind.

Lema 11 (Dedekind). *Sean $\sigma_1, \ldots, \sigma_n : E \to \mathbb{C}$ son diferentes inmersiones de un cuerpo de números E. Si $a_1, \ldots, a_n \in \mathbb{C}$ son tales que $\sum_{i=1}^n a_i \sigma_i(\alpha) = 0$ para todo $\alpha \in E$, entonces $a_1 = \cdots = a_n = 0$.*

Demostración. Procedemos por inducción en n. Si $n = 1$, tenemos la igualdad $0 = a_1\sigma_1(1) = a_1$ que prueba el lema. Supongamos entonces $n > 1$ y que el lema es cierto para el caso de $n-1$ inmersiones complejas E. Si $a_1 = 0$, el resultado se deduce de la hipótesis de inducción. Veamos que la alternativa no se puede dar, así que supongamos que $a_1 \neq 0$.

Poniendo $b_j = -a_j a_1^{-1}$, tendremos la igualdad

$$\sigma_1(\alpha) = \sum_{j=2}^n b_j \sigma_j(\alpha) = b_2\sigma_2(\alpha) + \cdots + b_n\sigma_n(\alpha), \quad \text{para todo } \alpha \in E.$$

Siendo $\alpha, \beta \in E$ cualesquiera dos elementos, puesto que $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$, tenemos por un lado la igualdad

$$\sigma_1(\alpha\beta) = \sum_{j=2}^n b_j \sigma_j(\alpha)\sigma_j(\beta) = b_2\sigma_2(\alpha)\sigma_2(\beta) + \cdots + b_n\sigma_n(\alpha)\sigma_n(\beta),$$

y por otro lado, puesto que $\sigma_1(\alpha\beta) = \sigma_1(\alpha)\sigma_1(\beta)$, tenemos la igualdad

$$\sigma_1(\alpha\beta) = \sum_{j=2}^n b_j \sigma_j(\alpha)\sigma_1(\beta) = b_2\sigma_2(\alpha)\sigma_1(\beta) + \cdots + b_n\sigma_n(\alpha)\sigma_1(\beta)\,.$$

Restando ambas expresiones, obtenemos que para todo $\alpha, \beta \in E$ se da la igualdad

$$0 = \sum_{j=2}^n b_j\big(\sigma_j(\beta) - \sigma_1(\beta)\big)\sigma_j(\alpha) = b_2\big(\sigma_2(\beta) - \sigma_1(\beta)\big)\sigma_2(\alpha) + \cdots + b_n\big(\sigma_n(\beta) - \sigma_1(\beta)\big)\sigma_n(\alpha).$$

Como es para todo $\alpha \in E$, aplicando la hipótesis de inducción, concluimos que ha de ser $b_j\big(\sigma_j(\beta) - \sigma_1(\beta)\big) = 0$, y esto para cualquier $\beta \in E$. Pero, como las inmersiones son diferentes, para cada $j = 2, \cdots, n$ es posible encontrar un $\beta \in E$ tal que $\sigma_j(\beta) \neq \sigma_1(\beta)$ y concluimos que ha de ser $b_j = 0$ para todo $j = 2, \cdots, n$. Esto nos lleva a que $\sigma_1(\alpha) = 0$ para todo $\alpha \in E$, lo que imposible ya que $\sigma_1(1) = 1$. $\square$

El siguiente Teorema de Lagrange muestra que, en presencia de adecuadas raíces de la unidad en el cuerpo base, una extensión es radical si y solo si es cíclica.

Teorema 12. * *Sea E/K una extensión finita de cuerpos de números, donde $\mathbb{C}_n \subseteq K$ ($\sim z_n \in K$). Son equivalentes:*
(1) E es una extensión radical de K generada por una raíz n-ésima de un elemento de K.
(2) E/K es una extensión cíclica y de grado un divisor de n.

Demostración. (1) $\Rightarrow$ (2): Por hipótesis $E = K(\sqrt[n]{a}z)$, para algún $a \in K$ y algún $z \in \mathbb{C}_n$. Como $z \in K$, resulta que $E = K(\sqrt[n]{a})$. Además, como el cuerpo de descomposición del polinomio $x^n - a$ sobre K es $K(\{\sqrt[n]{a}z,\, z \in \mathbb{C}_n\}) = K(\sqrt[n]{a}) = E$, ya que $\mathbb{C}_n \subseteq K$, la extensión E/K es normal.

Ahora, cada $\sigma \in G(E/K)$ está determinado por quien sea $\sigma(\sqrt[n]{a})$, que sabemos ha de ser otra raíz del polinomio $(x^n - a)^\sigma = x^n - a$. Así que que ha de ser $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\, z$ para algún $z \in \mathbb{C}_n$. Tenemos entonces una aplicación inyectiva

$$f : G(E/K) \to \mathbb{C}_n, \quad \sigma \mapsto f(\sigma) = z \ \text{ si } \ \sigma(\sqrt[n]{a}) = \sqrt[n]{a}\, z\, .$$

Esta aplicación es realmente un monomorfismo de grupos, pues si $\sigma' \in G(E/K)$ es tal que $\sigma'(\sqrt[n]{a}) = \sqrt[n]{a}z'$, entonces

$$\sigma\sigma'(\sqrt[n]{a}) = \sigma(\sqrt[n]{a}z') = \sigma(\sqrt[n]{a})\sigma'(z') = \sqrt[n]{a}\, zz'\ ,$$

de manera que $f(\sigma\sigma') = zz' = f(\sigma)f\sigma')$. El grupo $G(E/K)$ es entonces isomorfo a un subgrupo del grupo cíclico $\mathbb{C}_n$ y por tanto también cíclico y de orden un divisor de $n = |\mathbb{C}_n|$.

(2) $\Rightarrow$ (1): Supongamos que E/K es normal, con $[E : K] = d$, donde $d \mid n$, y que $G(E/K)$ es un grupo cíclico generado por σ. Notemos que la hipótesis de que $\mathbb{C}_n \subseteq K$ implica que $\mathbb{C}_d \subseteq K$. De hecho, si $n = dd'$, entonces $z_n^{d'} = e^{i\frac{2\pi d'}{dd'}} = e^{i\frac{2\pi}{d}} = z_d$ y $z_d \in K$. Para cada $x \in E$, formemos el elemento de E, llamado su **resolvente de Lagrange**,

$$\alpha_x = x + \sigma(x)z_d^{d-1} + \sigma^2(x)z_d^{d-2} + \cdots + \sigma^{d-1}(x)z_d\, .$$

Por el Lema de independencia de Dedekind, ha de ser $\alpha_x \neq 0$ para algún $x \in E$. Fijemos un tal x y sea $\alpha = \alpha_x$. Observamos entonces que

$$\begin{aligned} \sigma(\alpha) &= \sigma(x) + \sigma^2(x)z_d^{d-1} + \sigma^3(x)z_d^{d-2} + \cdots + \sigma^{d-1}(x)z_d^2 + \sigma^d(x)z_d \\ &= \sigma(x)z_d^d + \sigma^2(x)z_d^{d-1} + \sigma^3(x)z_d^{d-2} + \cdots + \sigma^{d-1}(x)z_d^2 + xz_d \\ &= z_d\Big(x + \sigma(x)z_d^{d-1} + \sigma^2(x)z_d^{d-2} + \cdots + \sigma^{d-1}(x)z_d\Big) \\ &= \alpha\, z_d. \end{aligned}$$

Así $0 \neq \alpha \in E$ y $\sigma(\alpha) = z_d\alpha$.

Vemos entonces, recursivamente, que $\sigma^k(\alpha) = z_d^k\alpha$, lo que nos lleva a que $\sigma^k(\alpha) \neq \alpha$, para $k = 1, \ldots, d-1$. Pero entonces $G(E/K(\alpha)) = \{id\} = G(E/E)$ y concluimos por el Teorema Fundamental de la Teoría de Galois, concluimos que $E = K(\alpha)$.

Vemos finalmente que $\sigma(\alpha^n) = \sigma(\alpha)^n = z_d^n\alpha^n = \alpha^n$, ya que $z_d^n = 1$ al ser d un divisor de n. De manera que $\alpha^n \in E^{G(E/K)} = K$, y concluimos que, efectivamente, la extensión E/K es radical y está generada por una raíz n-ésima de un elemento de K.