AYUDANTÍA XIX

GRUPOS Y ANILLOS (PRIMAVERA 2016)

En esta ayudantía estudiaremos la multiplicitivadad del grado en extensiones de cuerpos y calcularemos inversos multiplicativos en ciertos cuerpos.

1.- **Problema 1:**
Calcule el inverso multiplicativo de $1 + \sqrt[3]{2} + \sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$.

Desarrollo: Recordemos que por lo visto en la ayudantía XVII tenemos que $\phi : \mathbb{Q}[x]/(x^3 - 2) \to \mathbb{Q}(\sqrt[3]{2})$, $\phi(x) = \sqrt[3]{2}$ es un isomorfismo. Bajo este mismo tenemos que $\phi^{-1}(1 + \sqrt[3]{2} + \sqrt[3]{4}) = 1 + x + x^2$. Aplicando algoritmo de división obtenemos que $1 = (x - 1)(x^2 + x + 1) - (x^3 - 2)$. Por lo tanto, si aplicamos ϕ, obtenemos $1 = (\sqrt[3]{2} - 1)(\sqrt[3]{4} + \sqrt[3]{2} + 1)$. Luego $(\sqrt[3]{4} + \sqrt[3]{2} + 1)^{-1} = \sqrt[3]{2} - 1$.

i.- **Ejercicio:** Demuestre que el inverso de $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ es $\frac{a-b\sqrt{D}}{a^2-b^2D}$.

2.- **Problema 2:**
Demuestre cada una de las siguientes aseveraciones:
i.- Sea $K = \mathbb{Q}(i, \sqrt{2})$. Pruebe que $[K : \mathbb{Q}] = 4$.
ii.- Sea $L = \mathbb{Q}(\sqrt{3}, \sqrt{2})$. Pruebe que $[L : \mathbb{Q}] = 4$.

Desarrollo:
i.- Sabemos que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(x^2 - 2) = 2$. Por otro lado $K = \mathbb{Q}(\sqrt{2})(i)$, donde $p(x) = x^2 + 1 \in \mathbb{Q}(\sqrt{2})[x]$ es un polinomio que se anula en i. Por lo tanto $[K : \mathbb{Q}(\sqrt{2})] = 1$ o 2. Si $[K : \mathbb{Q}(\sqrt{2})] = 1$ entonces $K = \mathbb{Q}(\sqrt{2})$. Luego $i \in \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, lo que nos lleva a una constradicción. Por lo tanto $[K : \mathbb{Q}(\sqrt{2})] = 2$. Luego $[K : \mathbb{Q}] = 4$.
ii.- Sabemos que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(x^2-2) = 2$. Por otro lado $L = \mathbb{Q}(\sqrt{2})(\sqrt{3})$, donde $p(x) = x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$ es un polinomio que se anula en i. Por lo tanto $[L : \mathbb{Q}(\sqrt{2})] = 1$ o 2. Si $[L : \mathbb{Q}(\sqrt{2})] = 1$ entonces $L = \mathbb{Q}(\sqrt{2})$. Luego $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Esto en particular nos dice que existe $z \in \mathbb{Q}(\sqrt{2})$ tal que $z^2 = 3$. Pero todo elemento $z \in \mathbb{Q}(\sqrt{2})$ es de la forma $a + b\sqrt{2}$, para $a, b \in \mathbb{Q}$, esto ya que $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2) = \mathbb{Q} \oplus \mathbb{Q}\overline{x}$. Por lo tanto tenemos que $a^2 + 2b^2 + 2ab\sqrt{2} = 3$, es decir $a = 0$ o $b = 0$ y $a^2 + 2b^2 = 3$, para $a, b \in \mathbb{Q}$. Por ello tenemos que $3 \in \mathbb{Q}^2$ o $\frac{3}{2} \in \mathbb{Q}^2$, esto nos lleva a una contradicción. Por lo tanto $[L : \mathbb{Q}(\sqrt{2})] = 2$. Luego $[L : \mathbb{Q}] = 4$.

2.- **Ejercicio:** Calcule el grado sobre $\mathbb{Q}$ de la extensión $L = \mathbb{Q}(w, \sqrt[3]{2})$, donde $w = e^{\frac{2\pi i}{3}}$.

3.- **Problema 3:**
Sea L una extensión de K finitamente generada.

i.- Pruebe que si todo elemento en L satisface un polinomio mónico sobre K, entonces $[L : K] < \infty$.

ii.- Concluya que $L = \mathbb{Q}(\sqrt[n]{2} : n \in \mathbb{N}) \subset \mathbb{C}$ no es una extensión finitamente generada de $\mathbb{Q}$. Puede asumir que en esta extensión todos los elementos satisfacen polinomios sobre $\mathbb{Q}$.

Desarrollo:

i.- Sabemos que $L = K(a_1, \cdots a_t)$, para ciertos $a_t \in L$. Por esto podemos generar la torre de cuerpos definida por $L_0 = K$ y $L_i = L_{i-1}(a_i)$. Entonces como todo elemento en L satiface un polinomio sobre K tenemos que $[L_i : L_{i-1}] = \deg(irr_{a_i,L_{i-1}}(x)) < \infty$. Por lo multiplicatividad de grado en torres tenemos que $[L : K] = \sqcap \deg(irr_{a_i,L_{i-1}}(x)) < \infty$.

ii.- Observe que $L_n = \mathbb{Q}(\sqrt[n]{2})$ es una subextensión de L sobre $\mathbb{Q}$. Por lo probado en la ayudantía XVIII tenemos que $[L_n : \mathbb{Q}] = n$. Por lo tanto $[L : \mathbb{Q}] < n$, para todo $n \in \mathbb{N}$. Luego $[L : K] = \infty$. Por [i] concluimos que $L = \mathbb{Q}(\sqrt[n]{2} : n \in \mathbb{N})$ no es una extensión finitamente generada de $\mathbb{Q}$.

4.- **Problema 4:**
Considere $\eta = e^{\frac{2\pi i}{5}} \in \mathbb{C}$. Asumiendo que $\phi_5(x) = x^4 + x^3 + x^2 + x + 1$ es un polinomio irreducible sobre $\mathbb{Q}$, demuestre lo siguiente:

i.- Pruebe que $\mathbb{Q}(\eta)$ es una extensión de grado 4 de $\mathbb{Q}$.

ii.- Pruebe que $\mathbb{Q}(\eta + \eta^{-1})$ es una extensión de grado 2 de $\mathbb{Q}$

iii.- Escriba $\mathbb{Q}(\eta + \eta^{-1}) = \mathbb{Q}(\sqrt{d})$, para cierto $d \in \mathbb{Z}$.

Desarrollo:

i.- Observe que η satisface la ecuación $x^5 - 1 = 0$. Pero como $\eta \neq 1$ tenemos que η satisface $\phi_5(x) = \frac{x^5-1}{x-1}$. Como este polinomio es irreducible, tenemos que $\phi_5(x) = irr_{\eta,\mathbb{Q}}(x)$. Luego $[\mathbb{Q}(\eta) : \mathbb{Q}] = deg(\phi_5(x)) = 4$.

ii.- Observe que $\mathbb{Q}(\eta) = \mathbb{Q}(\eta + \eta^{-1})(\eta)$, donde η satisface el polinomio $p(x) = x^2 - x(\eta+\eta^{-1}) + 1 \in \mathbb{Q}(\eta+\eta^{-1})[x]$. Por lo tanto $[\mathbb{Q}(\eta) : \mathbb{Q}(\eta+\eta^{-1})] = 1$ o 2. Si $[\mathbb{Q}(\eta) : \mathbb{Q}(\eta+\eta^{-1})] = 1$ entonces $\eta \in \mathbb{Q}(\eta+\eta^{-1})$, donde $\mathbb{Q}(\eta+\eta^{-1}) \subset \mathbb{R}$, puesto que $\eta + \eta^{-1} = \eta + \overline{\eta} \in \mathbb{R}$. Esto nos lleva a una contradicción. Por lo tanto $[\mathbb{Q}(\eta) : \mathbb{Q}(\eta + \eta^{-1})] = 2$. Luego $[\mathbb{Q}(\eta + \eta^{-1}) : \mathbb{Q}] = 2$.

iii.- Tenemos que $(\eta+\eta)^2 = \eta^2+2+\eta^3 = 1-\eta-\eta^{-1}$. Por lo tanto $\eta+\eta^{-1}$ satisface el polinomio $x^2 + x - 1$. Luego $\eta + \eta^{-1} = \frac{-1+\sqrt{5}}{2}$ o bien $\eta + \eta^{-1} = \frac{-1-\sqrt{5}}{2}$. En cualquier caso $\mathbb{Q}(\eta + \eta^{-1}) = \mathbb{Q}(\sqrt{5})$. Por ello $d = 5$.

4.- **Ejercicio:** Sea $\eta = e^{\frac{2\pi i}{5}}$. Encuentre el inverso de $1 + \eta$ en $\mathbb{Q}(\eta)$.