UNIVERSIDAD AUTÓNOMA "BENITO JUÁREZ" DE OAXACA

Teoría de números: tarea 5

Fecha de entrega: 17 de octubre 2018

EJERCICIO 1

Asumir el teorema de reciprocidad cuadrática. ¿Cuál de las siguientes ecuaciones es soluble?

$x^2 - 5 = 0 \pmod{227}$

$x^2 - 3 = 0 \pmod{163}$

$x^2 - 13 = 0 \pmod{67}$

Si alguna es soluble, ¿puedes listar las soluciones?

EJERCICIO 2

Mostrar que los polinomios ciclotómicos $\Phi_p(x) \in \mathbb{Q}[x]$, donde $p \in \mathbb{Z}$ es primo, son irreducibles sobre $\mathbb{Q}$.

EJERCICIO 3

Consideremos $\zeta_5 = e^{2\pi/5}$ raíz del polinomio ciclotómico $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$. Mostrar que Φ_5 es soluble por radicales. Es decir,

$$\begin{aligned}\zeta_5 &= \cos(2\pi/5) + i\sin(2\pi/5)\\ &= \frac{\sqrt{5}-1}{4} + \frac{i}{2}\sqrt{\frac{5+\sqrt{5}}{2}}.\end{aligned}$$

EJERCICIO 4

Consideremos $\zeta_5 = e^{2\pi i/5}$. Escribir una base para $V = \mathbb{Q}(\zeta_5)$ como espacio vectorial sobre $\mathbb{Q}$. Dado que $V \subset \mathbb{C}$, considere la conjugación compleja $T : V \to V$ definida por $z \mapsto \overline{z}$. Con respecto a la base de arriba, ¿ cual es la matriz de T? ¿Es T un automorfismo de $\mathbb{Q}$-álgebras?

EJERCICIO 5

Consideremos ζ_5 y V como en el ejercicio anterior. Mostrar que $T_r : V \to V$, inducido por $\zeta_5 \to \zeta_5^r$, con $1 \leq r < 5$, es un automorfismo de $\mathbb{Q}$-álgebras. Si T es la aplicación del ejercicio anterior, ¿es $T = T_r$ para algún r?.

ARGUMENTAR A FAVOR O EN CONTRA

Con ζ_5 la raíz primitiva del ejercicio anterior, consideremos el anillo

$$\mathcal{O}(5) = \mathbb{Z} + \zeta_5\mathbb{Z} + \zeta_5^2\mathbb{Z} + \zeta_5^3\mathbb{Z}.$$

Un entero $p \in \mathbb{Z}$ primo factoriza en el anillo $\mathcal{O}(5)$ si y sólo si -5 es residuo cuadrático en $\mathbb{Z}/p$. *Pista: hacer ejemplos.*

ARGUMENTAR[1]

¿Para qué primos $p \in \mathbb{Z}$ es el polinomio $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}/p[x]$ irreducible?

¿Para qué primos $p \in \mathbb{Z}$ es el polinomio $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + +x + 1 \in \mathbb{Z}/p[x]$ irreducible?

[1] Pista: ¿Notas una relación con residuos cuadráticos?