ALGEBRA II

Licenciatura en Ciencias Matemáticas

1. Probar que para todo número natural n, la expresión

$$n^5 - n$$

es divisible por 10.

Solución.

Hemos de comprobar que $n^5 - n$ es múltiplo de 2 y de 5.

Vemos en primer lugar que es múltiplo de 2:

$$\begin{aligned} \text{si } n &\equiv 0 \operatorname{mod}(2) \text{ entonces } n^5 - n \equiv 0 - 0 \equiv 0 \operatorname{mod}(2), \\ \text{y si } n &\equiv 1 \operatorname{mod}(2) \text{ entonces } n^5 - n \equiv 1^5 - 1 \equiv 0 \operatorname{mod}(2). \end{aligned}$$

Por otra parte por el teorema de Fermat $n^5 - n \equiv 0 \operatorname{mod}(5)$, y con ello se concluye.

2. Probar que si p es primo y $p \equiv 1 \operatorname{mod}(4)$, entonces la ecuación:

$$y^2 + 1 \equiv 0 \operatorname{mod}(p)$$

tiene solución.

Solución.

El problema es muy similar a [GR,12] tal y como está rehecho en el foro.

Como 4 divide al orden $p-1$ del grupo cíclico Z_p^*, existe en éste un elemento y de orden 4, con lo que podemos escribir

$$y^4 - 1 = (y^2 - 1)(y^2 + 1) \equiv 0 \operatorname{mod}(p).$$

De esta forma, como $y^2 - 1 \neq 0 \operatorname{mod}(p)$ - ya que el orden de y es 4 y no 2 -, forzosamente tendremos

$$y^2 + 1 \equiv 0 \operatorname{mod}(p).$$

3. Sea u una raíz en $\mathbb{R}$ del polinomio $f(T) = T^3 - T^2 + T + 1$.

a) Calcular razonadamente el grado $[\mathbb{Q}(u) : \mathbb{Q}]$ y escribir una base de $\mathbb{Q}(u)$ como $\mathbb{Q}-$espacio vectorial que contenga a u.

b) Respecto de esta base, escribir la matriz del endomorfismo H "multiplicar por u":

$$\begin{array}{rcl} \mathbb{Q}(u) & \rightarrow & \mathbb{Q}(u) \\ H(v) & = & v \cdot u. \end{array}$$

c) Calular el polinomio característico de H y compararlo con f.

Solución.

El punto crucial reside en que el polinomio f es irreducible, que es lo que afirma [FL, 101]. De esta forma podemos escribir

$$[\mathbb{Q}(u) : \mathbb{Q}] = gr(f) = 3.$$

Esto implica directamente que una base de $Q(u)$ como $Q-$espacio vectorial es $\{1, u, u^2\}$ (ya que estos tres vectores son linealmente independientes, pues u no puede ser anulado por un polinomio de grado 2, ya que su polinomio mínimo es f).

Calculemos ahora la matriz del endomorfismo H respecto de esta base. Tenemos $H(1) = u, H(u) = u^2$ y $H(u^2) = u^3$. Como $u^3 - u^2 + u + 1 = 0$, podemos escribir al fin $H(u^2) = u^2 - u - 1$. Puestas estas imágenes en columnas, esccribimos:

$$\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix},$$

cuyo polinomio característico es

$$\begin{vmatrix} -T & 0 & -1 \\ 1 & -T & -1 \\ 0 & 1 & 1-T \end{vmatrix} = -T^3 + T^2 - T - 1,$$

que es precisamente $-f(T)$.

4. Consideremos las extensiones finitas de cuerpos:

$$K \hookrightarrow L \hookrightarrow E$$

donde E/K es de Galois. Probar que si L/K es también de Galois, entonces todo automorfismo $\phi \in G(E : K)$ verifica

$$\phi(L) \subseteq L.$$

Solución.

Es la implicación $(1) \Longrightarrow (*)$ en la demostración de la proposición 2.7 (Teorema fundamental de la teoría de Galois) pág. 324.