Tarea núm. 1 - soluciones (algunas)

Del libro de M. Artin - Algebra - cap. 13.

1.2. Sea $K \subset \mathbb{C}$ un subcampo no contenido en $\mathbb{R}$. Demuestra que K es denso en $\mathbb{C}$.

▷ Primero un lema: si $f : \mathbb{R}^n \to \mathbb{R}^m$ es una función contínua suprayectiva y $S \subset \mathbb{R}^n$ es denso, entonces $f(S) \subset \mathbb{R}^m$ es denso tambien. Demostración: sea $w \in \mathbb{R}^m$ y $\epsilon > 0$. Tenemos que demostrar que existe un $s \in S$ tal que $\|f(s) - w\| < \epsilon$. Sea B_ϵ la bola abierta con radio ϵ centrada en w. Como f es contínua, $f^{-1}(B_\epsilon)$ (la imagen inversa de B_ϵ bajo f) es abierta, y no vacía porque f es sobre. Así que existe un $s \in S \cap f^{-1}B_\epsilon$, por lo que $f(s) \in B_\epsilon$, o sea $\|f(s) - w\| < \epsilon$. QED

Ahora suponemos que existe un elemento $z = a + ib \in K$ con $b \neq 0$. Definimos $T : \mathbb{R}^2 \to \mathbb{R}^2$ por $T(x, y) = xz - y$. Entonces es facil verificar que T es una transformación lineal y que $det(T) = b \neq 0$, por lo que T es contínua y suprayectiva. Por el lema, la imagen de $\mathbb{Q}^2$ bajo T es densa en $\mathbb{C}$. Pero esta imagen está en K, ya que $\mathbb{Q} \subset K$ y $x, y, z \in K \implies xz - y \in K$ (por ser un campo). □

1.3. Sea R un dominio entero, $F \subset R$ un campo tal que $dim_F(R) < \infty$. Demuestra que R es un campo.

▷ Para cada $r \in R$, $r \neq 0$, sea $T_r : R \to R$ dado por $T_r(x) = rx$. Entonces T_r es F-lineal y su kernel es trivial ya que $rx = 0$, $r \neq 0$, implica $x = 0$ en un dominio entero. Como R tiene F-dimensión finita, T_r es sobre, por lo que existe un $x \in R$ tal que $rx = 1$.

Otra solución (más constructiva): sea $d = dim_F(R)$. Dado un $r \in R$, $r \neq 0$, los $d+1$ elementos $1, r, r^2, \ldots, r^d$ son linealmente dependientes, por lo que existen $c_0, c_1, \ldots, c_d \in F$, no todos 0, tal que $c_0 + c_1 r + \cdots + c_n r^d = 0$. Sea c_m el primer $c_i \neq 0$. Dividiendo $c_m r^m + c_{m+1} r^{m+1} + \cdots + c_d r^d = 0$ entre $c_m r^m$ y rearreglando obtenemos $1 = -r(c_{m+1} + c_{m+2} r + \cdots + c_n r^{n-m-1})/c_m$, por lo que $r^{-1} = -(c_{m+1} + c_{m+2} r + \cdots + c_n r^{n-m-1})/c_m$. □

1.4. Cierto o falso: un campo con 8 elementos tiene característica 2.

▷ Cierto. Mas general: el número de elementos de un campo finito K de característica p es una potencia de p. Demostración: K contiene una copia de $\mathbb{Z}_p$, así que es un espacio vectorial de dimensión finita, digamos d, sobre $\mathbb{Z}_p$, por lo que tiene p^d elementos. □

Nota: más tarde en el curso veremos que tal campo es único (salvo isomorfismo), y se puede construir como $\mathbb{Z}_2[x]$ módulo el ideal generado por un polinomio irreducible de grado 3, digamos $x^3 + x + 1$.

2.1 Sea α la raíz cúbica real de 2. Encuentra el polinómio irreducible de $1 + \alpha^2$ sobre $\mathbb{Q}$.

▷ Sea $\beta = 1 + \alpha^2$. Como $\beta \in \mathbb{Q}[\alpha]$ y α tiene grado 3, entonces β tiene grado 3 o 1. Pero β no puede tener grado 1, porque esto implica que es racional y que α tiene grado ≤ 2, así que β tiene grado 3. Así que *cualquer* polinomio $f \in \mathbb{Q}[x]$ de grado 3 tal que $f(\beta) = 0$ es automáticamente irreducible. Ahora $\beta - 1 = \alpha^2 \implies (\beta - 1)^3 = \alpha^6 = 4 \implies$ el polinomio buscado es $(x - 1)^3 - 4 = x^3 - 3x^2 + 3x - 5$. □

2.2. Si α es un elemento algebraico sobre un campo F con polinomio irreducible $f(x)$ de grado n, entonces $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $F[\alpha]$.

▷ Si $f(x)$ es un polinomio de grado n tal que $f(\alpha) = 0$ entonces se puede usarlo para expresar cualquer potencia de α como combinación lineal de $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, por lo que estos n elementos generan linealmente a $F[\alpha]$. Son linealmente independients porque de otro modo tendremos que α satisface una ecuación polinomial de grado menor que n, lo cual contradice la minimalidad de f. □

2.3 Determina el polinomio irreducible de $\alpha = \sqrt{3} + \sqrt{5}$ sobre cada uno de los siguientes campos:

(a) $\mathbb{Q}$.

▷ Primero demostramos que $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\alpha)$. Tenemos que $\alpha = \sqrt{3} + \sqrt{5} \implies \alpha^3 = 18\sqrt{3} + 14\sqrt{5}$. Luego, como los vectores $(1,1), (14,18) \in \mathbb{Q}^2$ son linealmente independientes, existen $x, y \in \mathbb{Q}$ tal que $x(1,1) + y(14,18) = (0,1) \implies x\alpha + y\alpha^3 \in \sqrt{5} \implies \sqrt{5} \in \mathbb{Q}(\alpha) \implies \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\alpha)$.

Ahora consideramos la sucesión de extensiones $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\alpha)$. La extensión $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ es de grado 2 y α es de grado 2 sobre $\mathbb{Q}(\sqrt{5})$ (ver inciso (b)) $\implies$ $\mathbb{Q}(\alpha)/\mathbb{Q}$ es de grado $2 \cdot 2 = 4$. Basta entonces encontrar un polinomio mónico de grado 4 en $\mathbb{Q}[x]$ que anula a α. Ahora $(\alpha - \sqrt{3})^2 = 5 \implies \alpha^2 - 2 = 2\sqrt{3}\alpha \implies (\alpha^2 - 2)^2 = 12\alpha^2 \implies$ el polinomio buscado es $(x^2 - 2)^2 - 12x^2 = x^4 - 16x^2 + 4$. □

(b) $\mathbb{Q}(\sqrt{5})$.

▷ Tenemos que $(\alpha - \sqrt{5})^2 = 3$ por lo que α es de grado ≤ 2 sobre $\mathbb{Q}(\sqrt{5})$. Luego α no es de grado 1 sobre $\mathbb{Q}(\sqrt{5})$ porque si $\sqrt{3} + \sqrt{5} = a + b\sqrt{5}$, $a, b, \in \mathbb{Q} \implies \sqrt{3} = a + (b-1)\sqrt{5} \implies 3 = a^2 + 5(b-1)^2 + 2a(b-1)\sqrt{5} \implies \sqrt{5} \in \mathbb{Q} \implies$ conradicción. (El caso de $a = 0$ o $b = 1$ se elimina tambien facilmente). Así que α es de grado 2 sobre $\mathbb{Q}[\sqrt{5}]$ y el polinomio buscado es $(x - \sqrt{5})^2 - 3 = x^2 - 2\sqrt{5}x + 2$. □

(c) $\mathbb{Q}(\sqrt{10})$.

▷ Tenemos que $\sqrt{10} \notin \mathbb{Q}(\alpha)$, por un argumento similar al inciso anterior $\implies$ $\sqrt{10}$ es de grado 2 sobre $\mathbb{Q}(\alpha) \implies [\mathbb{Q}(\alpha, \sqrt{10}) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt{10}) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$. Luego $[\mathbb{Q}(\sqrt{10}) : \mathbb{Q}] = 2 \implies [\mathbb{Q}(\alpha, \sqrt{10}) : \mathbb{Q}(\sqrt{10})] = 8/2 = 4 \implies \alpha$ es de grado 4 sobre $\mathbb{Q}(\sqrt{10}) \implies \alpha$ tiene el mismo polinomio irreducible sobre $\mathbb{Q}(\sqrt{10})$ que tiene sobre $\mathbb{Q}$. □

(d) $\mathbb{Q}[\sqrt{15}]$.

▷ Tenemos que $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{3}, \sqrt{5}]$ es de grado 4 sobre $\mathbb{Q}$ y $\sqrt{15}$ es de grado 2 sobre $\mathbb{Q} \implies \mathbb{Q}[\alpha]$ es de grado 2 sobre $\mathbb{Q}[\sqrt{15}]$. Luego $\alpha^2 = 8 + 2\sqrt{15}$ por lo que el polinomio buscado es $x^2 - (8 + 2\sqrt{15})$. □

4. Sea α una raiz compleja del polinomio irreducible $x^3 - 3x + 4$. Encuentra la inversa de $\alpha^2 + \alpha + 1$ in $\mathbb{Q}(\alpha)$ explicitamente, en la forma $a + b\alpha + c\alpha^2$.

▷ Idea: $(\alpha^2 + \alpha + 1)^{-1} = (\alpha - 1)/(\alpha^3 - 1) = (\alpha - 1)/(3\alpha - 5)$ por lo que basta enconrar la inversa de $3\alpha - 5$, digamos $a' + b'\alpha + c'\alpha^2$. Luego igualando coeficientes de las potencias de α en la igualdad $1 = (a' + b'\alpha + c'\alpha^2)(3\alpha - 5)$ se obtiene un sistema de ecuaciones lineales para a', b', c'. □

6. Demuestra que -1 no es una suma de cuadrados en $\mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$.

▷ El inciso es obvio para $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$. Pero ambos $\sqrt[3]{2}$ y $e^{2\pi i/3}\sqrt[3]{2}$ son raices del polinomio irreducible $x^3 - 2$, por lo que generan extensiones isomorfas de $\mathbb{Q}$. □