Ma31a Elementos de Álgebra **15 de Noviembre de 2008**

Pauta Control 3

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: E. Araya, O. Rivera*

PROBLEMA 1:

(i).- En $\mathbb{C}[x]$ el polinomio $p(x)$ tiene raíces $\pm 1 \pm i$, que en notación polar corresponde a $\alpha_k = \sqrt{2}e^{i(\pi/4+k\pi/2)}$ con $k = 0,\ldots,3$. Observar que $\alpha_k = \alpha_0^{2k+1}/2^k \in \mathbb{Q}(\alpha_0)$. Por otro lado, $\alpha_0 \notin \mathbb{Q}$ es raíz de x^2+2x+1, luego su grado algebraico sobre $\mathbb{Q}$ es 2. Como $p(x)$ tiene sus cuatro raíces reales en $\mathbb{Q}(\alpha_0)$, se descompone como producto de factores lineales en $\mathbb{Q}(\alpha_0)$. Sigue que si $\mathbb{K}$ es el cuerpo de descomposición para $p(x)$, entonces $\mathbb{K} \subseteq \mathbb{Q}(\alpha_0)$ y $2 \geq [\mathbb{Q}(\alpha_0):\mathbb{Q}] \geq [\mathbb{K}:\mathbb{Q}] > 1$, donde la última desigualdad es consecuencia del hecho que $p(x)$ no tiene raíces en $\mathbb{Q}$, por lo que $\mathbb{Q} \subsetneq \mathbb{K}$. Sigue que $\mathbb{K} = \mathbb{Q}(\alpha_0)$ y que $[\mathbb{K}:\mathbb{Q}] = 2$.

(ii).- Sea $p_1(x) = x^3+x+1$ y $p_2(x) = x^2+x+1$. Sea $\mathbb{K}$ el cuerpo de descomposición de $p(x) = p_1(x)p_2(x) \in \mathbb{F}_2[x]$. Notar que $\mathbb{K}$ contiene copias isomorfas de los cuerpos de descomposición de $p_1(x)$ y $p_2(x)$, digamos $\mathbb{K}_1$ y $\mathbb{K}_2$ respectivamente. Como $p_i(x) \in \mathbb{F}_2[x]$ es irreducible, sigue que $[\mathbb{K}_1:\mathbb{F}_2] = 3$ y $[\mathbb{K}_2:\mathbb{F}_2] = 2$. Como $[\mathbb{K}_i:\mathbb{F}_2]$ es divisor de $[\mathbb{K}:\mathbb{F}_2]$, y 2 y 3 son primos relativos, se tiene que 6 es divisor de $[\mathbb{K}:\mathbb{F}_2]$, i.e. $[\mathbb{K}:\mathbb{F}_2] \geq 6$.

Sea $\alpha \in \mathbb{K}$ raíz de $p_2(x)$. Se tiene que $\alpha^2 = \alpha+1$ y que $\mathbb{F}_2(\alpha) = \{0,1,\alpha,\alpha+1\}$. Notar que $p_1(0) = p_1(1) = 1$, $p_1(\alpha) = \alpha$, y $p_1(\alpha+1) = \alpha+1$. Como $p_1(x)$ es polinomio de grado cúbico y no tiene raíces en $\mathbb{F}_2(\alpha)$, entonces es irreducible en $\mathbb{F}_2(\alpha)[x]$. Sea $\beta \in \mathbb{K}$ raíz de $p_1(x)$. Observar que

$$p_1(x) = (x+\beta)(x^2+\beta x+\beta^2+1) = (x+\beta)(x+\beta^2)(x+\beta^2+\beta)\,.$$

Luego, $p_1(x)$ y $p_2(x)$, y por lo tanto también $p(x)$ se factorizan como producto de polinomios lineales en $\mathbb{F}_2(\alpha,\beta)[x]$. Además,

$$[\mathbb{F}_2(\alpha,\beta):\mathbb{F}_2] = [\mathbb{F}_2(\alpha,\beta):\mathbb{F}_2(\alpha)][\mathbb{F}_2(\alpha):\mathbb{F}_2] = 3\cdot 2 = 6\,.$$

Sigue que $\mathbb{K} = \mathbb{F}_2(\alpha,\beta)$.

(iii).- Sea $S = \{p(u)/q(u) \,:\, p,q \in \mathbb{F}[x], q(u) \neq 0\}$. Queremos probar que $S = \mathbb{F}(u)$.

Veamos que $\mathbb{F}(u) \subseteq S$. Se observa facilmente que S es cerrado para la suma, multiplicación e invirtiendo. Sin mayor dificultad se verifica que S es cuerpo. Como $\mathbb{F} \cup \{u\}$ está contenido

en S, el generado por $\mathbb{F} \cup \{u\}$, es decir $\mathbb{F}(u)$, está también contenido en S. En resumen, $\mathbb{F}(u) \subseteq S$.

Veamos ahora que $S \subseteq \mathbb{F}(u)$. En efecto, como $\mathbb{F} \cup \{u\}$ está contenido en $\mathbb{F}(u)$ que es cerrado para la suma y el producto, sigue que $p(u) \in \mathbb{F}(u)$ cualquiera que sea $p(x) \in \mathbb{F}[x]$. Como los inversos de los elementos no nulos de $\mathbb{F}(u)$ también están en $\mathbb{F}(u)$, y por cerradura del producto sobre $\mathbb{F}(u)$, se concluye que $S \subseteq \mathbb{F}(u)$.

(iv).- Si v es algebraico sobre $\mathbb{K}(u)$ entonces existe $s(x) \in \mathbb{K}(u)[x]$ tal que $s(v) = 0$. Digamos $s(x) = \sum_{i=1}^{n} s_i x^i$. Por (iii), cada coeficiente de s_i del polinomio $s(x)$ se puede escribir como $p_i(u)/q_i(u)$ donde $p_i(x), q_i(x) \in \mathbb{K}[x]$ y $q_i(u) \neq 0$. Como $s(v) = 0$, sigue que si $p_i'(x) = p_i(x) \prod_{j \neq i} q_j(x)$, entonces

$$s(v) = \sum_{i=1}^{n} \frac{p_i(u)}{q_i(u)} v^i = 0 \iff \sum_{i=1}^{n} p_i'(u) v^i = 0 \,.$$

Como $p_i'(x) \in \mathbb{K}[x]$, sigue que existen $c_{i,j}$'s en $\mathbb{K}$, todos nulos salvo por una cantidad finita, tales que

$$0 = \sum_{i,j \in \mathbb{N}} c_{i,j} u^j v^i = \sum_{j \in \mathbb{N}} \left(\sum_{i \in \mathbb{N}} c_{i,j} v^i \right) u^j \,.$$

Haciendo $q_j(v) = \sum_{i \in \mathbb{N}} c_{i,j} v^i$ se obtiene el polinomio $q(x) = \sum_{j \in \mathbb{N}} q_j(v) x^j \in \mathbb{K}(v)[x]$ tal que $q(u) = 0$, i.e. u es algebraico sobre $\mathbb{K}(v)$.

PROBLEMA 2:

(i).- Basta observar que toda clausura algebraica es normal.

(ii).- Supongamos que $\mathbb{N}|_{\mathbb{F}}$ es normal. Sea $p(x) \in \mathbb{F}[x]$ irreducible y $a \in \mathbb{N}$ raíz de $p(x)$. Sea $p_a(x) \in \mathbb{F}[x]$ polinomio minimal de a. Dado que $p(x)$ y $p_a(x)$ comparten una raíz en una extensión de $\mathbb{F}$ no pueden ser primos relativos. Pero como ambos son irreducibles en $\mathbb{F}[x]$ se debe tener que difieren en a lo más un factor constante. Como $p_a(x)$ se descompone como producto de polinomios lineales en $\mathbb{N}[x]$, lo mismo debe ocurrir para $p(x)$.

El converso se tiene trivialmente. En efecto, dado que $\mathbb{N}$ es algebraico sobre $\mathbb{F}$, entonces para cada $a \in \mathbb{N}$ existe un polinomio minimal $p_a(x) \in \mathbb{F}[x]$ para a. Por definición de polinomio minimal, se tiene que $p_a(x)$ es irreducible en $\mathbb{F}[x]$. Como $a \in \mathbb{N}$ es raíz de $p_a(x)$, por hipótesis sigue que $p_a(x)$ se factoriza como producto de polinomios lineales en $\mathbb{N}[x]$.

(iii).- Sea $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. Observar que $\sqrt[3]{2}$ es raíz irracional del polinomio cúbico $p(x) \in \mathbb{R}[x]$, luego $p(x)$ es irreducible en $\mathbb{Q}[x]$, y por lo tanto es polinomio minimal de $\sqrt[3]{2}$. Sin embargo, en $\mathbb{Q}(\sqrt[3]{2})$ el polinomio $p(x)$ se factoriza como

$$p(x) = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}) \,.$$

Es decir, $p(x)$ no se descompone como producto de factores lineales en $\mathbb{Q}(\sqrt[3]{2})$. Luego, $\mathbb{Q}(\sqrt[3]{2})$ no es normal.

(iv).- Observar primero que si $\mathbb{N}|_{\mathbb{F}}$ es normal, entonces $\mathbb{N}$ es algebraico sobre $\mathbb{F}$ y por lo tanto también sobre $\mathbb{K}$. Sigue que para cada $a \in \mathbb{N}$ existen $p(x)$ y $q(x)$ polinomios minimales en $\mathbb{F}[x]$ y $\mathbb{K}[x]$ respectivamente. Notar que $p(x), q(x) \in \mathbb{K}[x]$ comparten una raíz en una extensión de $\mathbb{K}$, a saber $a \in \mathbb{N}$. Sigue que para cada $a \in \mathbb{N}$, $p(x)$ y $q(x)$ no son primos relativos, pero como $q(x)$ es irreducible en $\mathbb{K}[x]$, necesariamente se debe tener que $q(x)|p(x)$. Como $p(x)$ se descompone como producto de factores lineales en $\mathbb{N}[x]$, entonces lo mismo se tiene para $q(x)$. En resumen, el polinomio minimal en $\mathbb{K}[x]$ de cualquier $a \in \mathbb{N}$ se factoriza como producto de polinomios lineales en $\mathbb{N}[x]$, i.e. $\mathbb{N}|_{\mathbb{K}}$ es normal.

(v).- Veremos primero que $\sigma(\mathbb{N}) \subseteq \mathbb{N}$. En efecto, sea $a \in \mathbb{N}$ y $p_a(x) \in \mathbb{F}[x]$ polinomio minimal de a. Dado que σ va sobre $\mathbb{F}$, se tiene que

$$p^{\sigma}(x) = \sum_{m \in \mathbb{N}} \sigma(p_m) x^m = p(x)\,.$$

Por otro lado, si $a = \alpha_0, \alpha_1, \ldots, \alpha_n \in \mathbb{N}$ son todas las raíces de $p_a(x)$ (con repeticiones) y como $\mathbb{N}|_{\mathbb{F}}$ es normal, se tiene que para algún $\lambda \in \mathbb{F}$,

$$p_a(x) = \lambda \prod_{i=0}^{n-1} (x - \alpha_i)\,.$$

Por otro lado, se verifica que

$$p_a^{\sigma}(x) = \lambda \prod_{i=0}^{n-1} (x - \sigma(\alpha_i))\,.$$

Luego,

$$\prod_{i=0}^{n-1} (x - \alpha_i) = \prod_{i=0}^{n-1} (x - \sigma(\alpha_i))\,,$$

y por lo tanto $\sigma(\alpha_i) \subseteq \{\alpha_0, \ldots, \alpha_{n-1}\} \subseteq \mathbb{N}$ cualquiera sea $i \in \mathbb{N}$, en particular $\sigma(a) \in \mathbb{N}$.

De la discusión anterior se concluye que $\sigma(\mathbb{N}) \subseteq \mathbb{N}$. Se tiene que $\mathbb{N}$ es algebraico sobre $\mathbb{F}$ y $\sigma : \mathbb{N} \to \mathbb{N}$ es un inmersión sobre $\mathbb{F}$. Por resultado visto, sigue que $\sigma : \mathbb{N} \to \mathbb{N}$ es un automorfismo, en particular $\sigma(\mathbb{N}) = \mathbb{N}$ como se quería demostrar.