Ma3101 Elementos de Álgebra	**15 de Noviembre de 2014**

Pauta Control 3

Prof. Cátedra: M. Kiwi — *Prof. Auxiliar: B. Ruiz, A. Turkieltaub*

PROBLEMA 1:

(i).- Por resultado visto $\mathbb{Q}(u)$ es un $\mathbb{Q}$-espacio vectorial con base $\{1,u,u^2\}$. Luego, como $u^3 = -3u-3$, sigue que $u^4 = -3u^2-3u$, por lo que

$$\begin{aligned} 1 &= (\alpha+\beta u+\gamma u^2)(7-2u+u^2) \\ &= 7\alpha+(7\beta-2\alpha)u+(\alpha-2\beta+7\gamma)u^2+(\beta-2\gamma)u^3+\gamma u^4 \\ &= 7\alpha-3(\beta-2\gamma)+(7\beta-2\alpha-3(\beta-2\gamma)-3\gamma)u+(\alpha-2\beta+7\gamma-3\gamma)u^2 \\ &= 7\alpha-3\beta+6\gamma+(-2\alpha+4\beta+3\gamma)u+(\alpha-2\beta+4\gamma)u^2. \end{aligned}$$

Como $\{1,u,u^2\}$ es una $\mathbb{Q}$-base, se tiene que

$$\begin{aligned} 7\alpha-3\beta+6\gamma &= 1, \\ -2\alpha+4\beta+3\gamma &= 0, \\ \alpha-2\beta+4\gamma &= 0. \end{aligned}$$

Resolviendo el sistema, sigue que $\alpha = \frac{2}{11}$, $\beta = \frac{1}{11}$, y $\gamma = 0$, i.e., $(7-2u+u^2)^{-1} = \frac{1}{11}(2+u)$.

(ii).- Dado que en $\mathbb{Z}_3$ tenemos que $f(0) = -1$, $f(1) = 1$, y $f(2) = 5 = 2$, sigue que f no admite raíces en $\mathbb{Z}_3$, y como es un polinomio de grado 2, necesariamente debe ser irreducible sobre $\mathbb{Z}_3$. Análogamente se verifica que x^2+1 es irreducible sobre $\mathbb{Z}_3$ por lo que $\mathbb{E} = \mathbb{Z}_3/(x^2+1)$ es una extensión de $\mathbb{Z}_3$ de grado 2. De hecho, $\mathbb{Z}_3$ es el cuerpo primo de $\mathbb{E}$, por lo que este último tiene característica 3, y por lo tanto la fórmula para las raíces de una ecuación cuadrática es aplicable. Observando que $\mathbb{Z}_3 \subset \mathbb{E}$ se tiene que $2^{-1} = 2 = -1$ y $5 = 2$ en $\mathbb{E}$, sigue que f admite en $\mathbb{E}$ las raíces,

$$\tfrac{1}{2}\big(-1 \pm \sqrt{1+4}\big) = 2\big(-1 \pm \sqrt{2}\big) = 1 \pm 2\sqrt{2},$$

donde $\sqrt{2}$ representa una raíz del polinomio irreducible $x^2+1 = x^2-2 \in \mathbb{Z}_3[x]$. Sigue que $\mathbb{Z}_3(\sqrt{2}) \cong \mathbb{E}$ por lo que las dos raíces indicadas están en $\mathbb{E}$.

(iii).- Como $\sqrt{2}$ es raíz de x^2-2, sigue que $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{3})]$ es a lo más 2, i.e., igual a 1 o 2. Veamos que se tiene el segundo caso. Por contradicción, si $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 1$, entonces $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{3})$. En particular $\sqrt{2}\in\mathbb{Q}(\sqrt{3})$ por lo que existirían $a,b\in\mathbb{Q}$ tales que $\sqrt{2}=a+b\sqrt{3}$. Elevando al cuadrado, tendríamos que $2=a^2+2ab\sqrt{3}+3b^2$ y al despejar obtendríamos que $\sqrt{3}\in\mathbb{Q}$, lo cual es una falacia.

Como además, $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2$, por resultado visto,

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=4.$$

Por otro lado, dado que $\sqrt{6}=\sqrt{2}\cdot\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$ tenemos que $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{6})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$, y por el mismo resultado visto previamente mencionado,

$$4=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{6})][\mathbb{Q}(\sqrt{6}):\mathbb{Q}]. \tag{1}$$

Pero, $[\mathbb{Q}(\sqrt{6}):\mathbb{Q}]=2$ (porque $\sqrt{6}$ es raíz del polinomio irreducible x^2-6). Sustituyendo en (1) y despejando, deducimos que $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{6})]=2$.

(iv).- Por contradicción, supongamos que $\alpha=uv$ y $\beta=u+v$ son algebráicos sobre $\mathbb{Q}$. Sigue que $u\beta=u^2+uv=u^2+\alpha$, i.e., $u^2-\beta u$ es algebráico sobre $\mathbb{Q}$. Luego, existe $P(x)\in\mathbb{Q}[x]$ polinomio tal que $P(u^2-\beta u)=0$. Pero, dado que la composición de polinomios es un polinomio, sigue que $Q(x)=P(x^2-\beta x)\in\mathbb{Q}(\beta)[x]$ tiene a u como raíz, i.e., u es algebráico sobre $\mathbb{Q}(\beta)$, y como β es alegebráico sobre $\mathbb{Q}$, por resultado visto, sigue que u es agebráico sobre $\mathbb{Q}$, obteniéndose una contradicción.

(v).- Observemos primero que $x^6-4=(x^3-2)(x^3+2)$. La única raíz en $\mathbb{R}$ de x^3-2 es $\sqrt[3]{2}$, que no es racional. Luego, x^3-2 es irreducible sobre $\mathbb{Q}$. Sus raíces en $\mathbb{C}$ son $\theta_0=\sqrt[3]{2}$, $\theta_1=\sqrt[3]{2}e^{i2\pi/3}$, y $\theta_2=\sqrt[3]{2}e^{-i2\pi/3}$. Como $\theta_2=\theta_1^2$, sigue que x^3-2 se descompone en factores lineales en $\mathbb{Q}(\theta_0,\theta_1)$. Por otro lado, las raíces de x^3+2 en $\mathbb{C}$ son $-\sqrt[3]{2}=-\theta_0$, $\sqrt[3]{2}e^{i\pi/3}=\theta_1+\theta_0$, y $\sqrt[3]{2}e^{-i\pi/3}=\theta_2+\theta_0$. Luego, están todas en $\mathbb{Q}(\theta_0,\theta_1)$. Como el cuerpo de descomposición $\mathbb{K}$ de x^6-4 debe contener θ_0 y θ_1, necesariamente se tiene que $\mathbb{Q}(\theta_0,\theta_1)\subseteq\mathbb{K}$. Como en $\mathbb{Q}(\theta_0,\theta_1)$ el polinomio x^6-4 se descompone en factores lineales, por minimalidad del cuerpo de descomposición, se tiene que $\mathbb{K}=\mathbb{Q}(\theta_0,\theta_1)$.

(vi).- Como α es raíz de $P(x)$ tenemos que $\alpha^4=1+\alpha+\alpha^2+\alpha^3$ y que $(x+\alpha)|P(x)$ (recordar que en $\mathbb{F}_2$ se tiene que $1=-1$). En particular,

$$P(x)=(x+\alpha)(x^3+(1+\alpha)x^2+(1+\alpha+\alpha^2)x+(1+\alpha+\alpha^2+\alpha^3)). \tag{2}$$

Necesitamos descomponer $Q(x)=x^3+(1+\alpha)x^2+(1+\alpha+\alpha^2)x+(1+\alpha+\alpha^2+\alpha^3)$ como producto de polinomios irreducibles en $\mathbb{F}_2(\alpha)$.

Como $\mathbb{F}_2$ es de característica 2, tenemos que $0=(P(\alpha))^2=P(\alpha^2)$ y análogamente $0=(P(\alpha^2))^2=P(\alpha^4)$. Sigue que $\alpha^2,\alpha^4\in\mathbb{F}_2(\alpha)$ también son raíces de $P(x)$, y luego también de $Q(x)$. Dividiendo, obtenemos que

$$Q(x)=(x+\alpha^2)(x^2+(1+\alpha+\alpha^2)x+\alpha^2)=(x+\alpha^2)(x+\alpha^4)(x+\alpha^3).$$

Luego, $P(x)$ se descompone sobre $\mathbb{F}_2(\alpha)$ como:

$$P(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+1+\alpha+\alpha^2+\alpha^3).$$

PROBLEMA 2:

(i.1).- Sea m el grado de $P(x)$. Sabemos que $\{1,\dots,a^{m-1}\}$ es una $\mathbb{F}$-base de $\mathbb{F}(a)$. Definimos τ_b por

$$\tau_b(\alpha_0+\alpha_1 a+\ldots+\alpha_{n-1}a^{n-1}) = \sigma(\alpha_0)+\sigma(\alpha_1)b+\ldots+\sigma(\alpha_{n-1})b^{n-1}.$$

Se verifica fácilmente que τ_b es un morfismo de cuerpos tal que $\tau_b(a) = b$ y $\tau_b|_{\mathbb{F}} = \sigma$.

Si $\tau : \mathbb{F}(a) \to \mathbb{K}$ es también morfismos de cuerpos tal que $\tau(a) = b = \tau_b(a)$ y $\tau|_{\mathbb{F}} = \sigma = \tau_b|_{\mathbb{F}}$, entonces como τ y τ_b son funciones $\mathbb{F}$-lineales que coinciden en una base del $\mathbb{F}$-espacio vectorial de dimensión finita $\mathbb{F}(a)$, deben ser idénticas.

(i.2).- Basta tomar $b = \tau(a)$, observar que

$$0 = \tau(0) = \tau(P(a)) = \sum_{n\in\mathbb{N}} \tau(p_n)b^n = \sum_{n\in\mathbb{N}} \sigma(p_n)b^n = P^{\sigma}(b),$$

y concluir usando la únicidad de la parte anterior.

(ii.1).- Si $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{E})$ y $a \in \mathbb{E}$ es raíz de $P(x)$, y dado que ahora $P^{\sigma}(x) = P(x)$,

$$0 = \sigma(0) = \sigma(P(a)) = P^{\sigma}(\sigma(a)) = P(\sigma(a)).$$

Luego, σ lleva las raíces en $\mathbb{E}$ de $P(x)$ en raíces de $P(x)$. Como σ es invertible, sigue que es permutación de $\{\alpha \in \mathbb{E} : P(\alpha) = 0\}$.

Consideremos ahora $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$. Como $\mathbb{Q}(\sqrt{2})$ es el cuerpo de descomposición de x^2-2 sobre $\mathbb{Q}$ con raíces $\pm\sqrt{2}$, por lo recién establecido, se debe tener que $\sigma(\sqrt{2}) = \sqrt{2}$ o $\sigma(\sqrt{2}) = -\sqrt{2}$. En cualquier caso, σ queda completamente determinado. En el primer caso, se verifica que $\sigma = id_{\mathbb{Q}}$. En el segundo caso, σ es el automorfismo que a $a+b\sqrt{2}$, $a,b \in \mathbb{Q}$, le asocia $a-b\sqrt{2}$.

Consideremos ahora $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$. Como $P(x) = x^3-2$ es polinomio irreducible sobre $\mathbb{Q}$, por la afirmación recién establecida, sigue que σ es una permutación de las raíces de $P(x)$ en $\mathbb{Q}(\sqrt[3]{2})$. Pero, $\sqrt[3]{2}$ es la única raíz de $P(x)$ en $\mathbb{Q}(\sqrt[3]{2})$, por lo que $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Dado que además σ fija $\mathbb{Q}$, de la parte (i.1) se concluye que existe un único morfismo con estas propiedades, que de hecho es $id_{\mathbb{Q}(\sqrt[3]{2})}$.

(ii.2).- Como todo morfismo de cuerpos es inyectivo, sólo hace falta mostrar que σ es sobreyectivo. Sea $b \in \mathbb{K}$, y sea $P(x) \in \mathbb{F}[x]$ su polinomio minimal (que existe porque $\mathbb{K}$ es algebráico sobre $\mathbb{F}$). Sean $a_1, \ldots, a_k$ todas las raíces distintas en $\mathbb{K}$ de $P(x)$. Como ya se vió en la parte anterior,

$$P(\sigma(a_i)) = P^{\sigma}(a_i) = P(a_i) = 0,$$

i.e., σ lleva raíces de $P(x)$ en raíces de $P(x)$. Como además σ fija $\mathbb{F}$, se tiene que $\sigma(\mathbb{F} \cup \{a_1, \ldots, a_k\}) \subseteq \mathbb{F} \cup \{a_1, \ldots, a_k\}$. Sigue que, $\sigma : \mathbb{F}(a_1, \ldots, a_k) \to \mathbb{F}(a_1, \ldots, a_k)$ es un morfismo de cuerpos (en particular inyectivo), i.e., es una función $\mathbb{F}$-lineal inyectiva entre $\mathbb{F}$-espacios vectoriales de (idéntica) dimensión finita. Luego, por Teorema Núcleo Imágen, $\sigma(\mathbb{F}(a_1, \ldots, a_k)) = \mathbb{F}(a_1, \ldots, a_k)$. Dado que b es raíz de $P(x)$, tenemos que $b \in \{a_1, \ldots, a_k\} \subset \mathbb{F}(a_1, \ldots, a_k)$, y por lo tanto debe existir $a \in \mathbb{F}(a_1, \ldots, a_k) \subseteq \mathbb{K}$ tal que $\sigma(a) = b$. Queda así demostrado que σ es sobreyectiva.

(ii.3).- Si $[\mathbb{E} : \mathbb{F}] = 1$, entonces $\mathbb{E} = \mathbb{F}$, y el único morfismo de cuerpos de $\mathbb{E}$ en $\mathbb{E}$ que fija $\mathbb{F}$ es $id_{\mathbb{E}}$. Luego, se tiene el caso base de la inducción. Supongamos que también se tiene la afirmación cuando $[\mathbb{E} : \mathbb{F}] = n > 1$. Sea $a \in \mathbb{E} \setminus \mathbb{F}$ raíz de $P(x)$, y supongamos que $P(x)$ tiene grado $m \neq 0$. De la parte (i.1) sabemos que $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{E})$ queda completamente determinado en $\mathbb{F}(a)$ por el valor $\sigma(a)$, el cual como se vió en la parte (ii.1), debe ser una raíz de $P(x)$, de las cuales hay a lo más $m = [\mathbb{F}(\alpha) : \mathbb{F}]$. Sigue que hay a lo más $[\mathbb{F}(\alpha) : \mathbb{F}]$ opciones posibles para extender un automorfismo σ que fija $\mathbb{F}$ a $\mathbb{F}(\alpha)$. Por hipótesis inductiva (dado que $\mathbb{E}$ sigue siendo cuerpo de descomposición de $P(x)$ sobre $\mathbb{F}(\alpha)$), cada una de estas extensiones puede a su vez extenderse de a lo más $[\mathbb{E} : \mathbb{F}(\alpha)]$ formas a $\mathbb{E}$. Luego,

$$|\mathrm{Aut}_{\mathbb{F}}(\mathbb{E})| \leq [\mathbb{E} : \mathbb{F}(\alpha)][\mathbb{F}(\alpha) : \mathbb{F}] = [\mathbb{E} : \mathbb{F}],$$

donde la última igualdad es un resultado visto en cátedras,