MA-31A Elementos de Álgebra	**6 de Diciembre, 2003**

Pauta Examen

Prof. Cátedra: M. Kiwi — *Prof. Auxiliar: H. Castro, J. Soto*

(i).- Basta ver que $\mathbf{Gal}(\mathbb{K}|_{\mathbb{F}})$ es subgrupo del grupo de automorfismos de $\mathbb{K}$. En efecto, $\mathbf{Gal}(\mathbb{K}|_{\mathbb{F}})$ es no vacío pues contiene $id_{\mathbb{K}}$. Además, si $\phi \in \mathbf{Gal}(\mathbb{K}|_{\mathbb{F}})$, entonces ϕ^{-1} es un automorfismo de $\mathbb{K}$ y como $\phi|_{\mathbb{F}} = id_{\mathbb{F}}$ también se tiene que $\phi^{-1}|_{\mathbb{F}} = id_{\mathbb{F}}$. Finalmente, sean $\phi, \theta \in \mathbf{Gal}(\mathbb{K}|_{\mathbb{F}})$. Como la composición de automorfismos es también un automorfismo y $(\phi \circ \theta)|_{\mathbb{F}} = \phi|_{\theta(\mathbb{F})} \circ \theta|_{\mathbb{F}} = \phi|_{\mathbb{F}} \circ id_{\mathbb{F}} = id_{\mathbb{F}}$, sigue que $\phi \circ \theta \in \mathbf{Gal}(\mathbb{K}|_{\mathbb{F}})$.

(ii).- Como $[\mathbb{K} : \mathbb{F}] = 2$, existe $P(x) = x^2 + bx + c \in \mathbb{F}[x]$ irreducible sobre $\mathbb{F}$ tal que $\mathbb{K} \cong \mathbb{F}[x]/(P) \cong \mathbb{F}(\alpha)$ donde $\alpha \in \mathbb{K}$ es raíz de P. Sea $\alpha' \in \mathbb{K}$ tal que $P(x) = (x - \alpha)(x - \alpha')$. Luego, $\alpha + \alpha' = b$. Si $\alpha = \alpha'$, entonces $\alpha \in \mathbb{F}$ contradiciendo el hecho que $\mathbb{F}(\alpha) = \mathbb{K} \neq \mathbb{F}$. Resumiendo, tenemos que $\alpha \neq \alpha'$. Observar que tampoco puede ocurrir que $\alpha' \in \mathbb{F}$ pues de la igualdad $\alpha + \alpha' = b$ se concluiría que $\alpha \in \mathbb{F}$, algo que sabemos no es cierto. Luego, $\mathbb{F} \subseteq \mathbb{F}(\alpha') \subseteq \mathbb{K}$ con $\mathbb{F} \neq \mathbb{F}(\alpha')$. Como $[\mathbb{K} : \mathbb{F}] = 2$ sigue fácilmente que $\mathbb{F}(\alpha') = \mathbb{K}$.

La observación crucial para obtener la conclusión deseada es que $x^2 - D$ con $D = b^2 - 4c$ no tiene raíces en $\mathbb{F}$. Para ver esto, observar que como $P(\alpha) = 0$, si $\delta = 2\alpha + b$, entonces

$$\delta^2 - D = 4\alpha^2 + 4\alpha b + b^2 - (b^2 - 4c) = 4(-b\alpha - c) + 4\alpha b + 4c = 0\,.$$

Luego, δ es raíz de $x^2 - D$ y no puede estar en $\mathbb{F}$ pues ello implicaría que $\alpha \in \mathbb{F}$. La otra raíz de $x^2 - D$ es claramente $-\delta$, es decir, $x^2 - D$ no posee raíces en $\mathbb{F}$.

Nuevamente, como $\delta \notin \mathbb{F}$ y $[\mathbb{K} : \mathbb{F}] = 2$, se tiene que $\mathbb{F}(\delta) = \mathbb{K}$.

(iii).- Notar que $\phi \in \mathbf{Gal}(\mathbb{K}|_{\mathbb{F}})$ implica en particular que ϕ es un automorfismo de $\mathbb{K}$ que va sobre $\mathbb{F}$. Luego, ϕ lleva raíces de $x^2 - D$ en raíces de $x^2 - D$. Como $x^2 - D$ sólo tiene dos raíces en $\mathbb{K}$, a saber $\pm\delta$, sólo hay dos posibilidades; (1) que $\phi(\delta) = \delta$, y (2) que $\phi(\delta) = -\delta$. Además, sabemos que $\phi(1) = 1$.

Por otro lado, como $\mathbb{K} = \mathbb{F}(\delta)$, el conjunto $\{1, \delta\}$ es una base de $\mathbb{K}$ como espacio vectorial sobre $\mathbb{F}$. De aquí que ϕ quede completamente definida una vez fijado los valores que toma en $\{1, \delta\}$. Luego, en el caso (1) de más arriba se debe tener necesariamente que $\phi = id$. En el caso (2) se tiene que $\phi = \sigma$. hemos concluido que $\mathbf{Gal}(\mathbb{K}|_{\mathbb{F}}) \subseteq \{id, \sigma\}$.

Por otro lado, id y σ están claramente en $\mathbf{Gal}(\mathbb{K}|_{\mathbb{F}})$.

(iv.1).- Como ϕ es un morfismo sobre $\mathbb{K} = \mathbb{F}(\alpha, \beta)$, está determinado por los valores que toma en $\{1, \alpha, \beta\}$. Pero $\phi(1) = 1$ siempre. Sigue que sólo hay cuatro posibilidades para ϕ, a saber:

$$\begin{array}{rclcrcl} \phi(\alpha) & = & \alpha & \text{y} & \phi(\beta) & = & \beta\,, \\ \phi(\alpha) & = & -\alpha & \text{y} & \phi(\beta) & = & \beta\,, \\ \phi(\alpha) & = & \alpha & \text{y} & \phi(\beta) & = & -\beta\,, \\ \phi(\alpha) & = & -\alpha & \text{y} & \phi(\beta) & = & -\beta\,. \end{array}$$

(iv.2).- Sea G el grupo de automorfismos generado por $\{\sigma, \tau\}$ Como $\{\sigma, \tau\} \subseteq \mathbf{Gal}(\mathbb{K}|_{\mathbb{F}})$, se tiene que $G \subseteq \mathbf{Gal}(\mathbb{K}|_{\mathbb{F}})$. Luego, del punto anterior concluimos que G tiene a lo más cuatro elementos. Por otro lado $\sigma \circ \tau(\alpha) = -\alpha$ y $\sigma \circ \tau(\beta) = -\beta$, por lo que $\sigma \circ \tau \notin \{id, \alpha, \tau\}$. Obviamente que $id, \sigma, \tau \in G$. Como además $\sigma \circ \tau \in G$, tenemos que $G = \mathbf{Gal}(\mathbb{K}|\mathbb{F}) = \{id, \sigma, \tau, \sigma \circ \tau\}$. Sigue que $|G| = [\mathbb{K} : \mathbb{F}]$, por lo que $\mathbb{K}|_{\mathbb{F}}$ es de Galois.

(v).- Sean $a, b \in \mathbb{K}$. Luego, $\varphi(a) = a$ y $\varphi(b) = b$ para todo $\varphi \in G$. Sigue que $\varphi(a \pm b) = a \pm b$ y $\varphi(ab) = ab$, i.e., $a \pm b$ y ab están en $\mathbb{K}^G$. Si $b \neq 0$, entonces $\varphi(b^{-1}) = (\varphi(b))^{-1} = b^{-1}$, i.e., nuevamente $b \in \mathbb{K}^G$. Se concluye que $\mathbb{K}^G$ es un subcuerpo de $\mathbb{K}$.

(vi).- Sea $\mathbb{L} = \mathbb{K}^G$. Entonces, $\mathbb{F} \subseteq \mathbb{L}$ por lo que cualquier $\mathbb{L}$-automorfismo de $\mathbb{K}$ es un $\mathbb{F}$-automorfismos de $\mathbb{K}$, i.e., $G \subseteq \mathbf{Gal}(\mathbb{K}|_{\mathbb{L}})$. Además, cualquier elemento de G es claramente un $\mathbb{L}$-automorfismo de $\mathbb{K}$. Se concluye que $G = \mathbf{Gal}(\mathbb{K}|_{\mathbb{L}})$. Pero, dado que $\mathbb{K}|_{\mathbb{F}}$ es una extensión de Galois, $o(G) = [\mathbb{K} : \mathbb{F}]$. Del Teorema 1 tenemos que $o(G)$ divide $[\mathbb{K} : \mathbb{L}]$, o sea $[\mathbb{K} : \mathbb{F}] \leq [\mathbb{K} : \mathbb{L}]$. Dado que $\mathbb{F} \subseteq \mathbb{L}$ sigue que $[\mathbb{K} : \mathbb{L}] \leq [\mathbb{K} : \mathbb{F}]$.

Resumiendo, $[\mathbb{K} : \mathbb{L}] = [\mathbb{K} : \mathbb{F}]$ y $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$. Se concluye que $\mathbb{F} = \mathbb{L}$.

(vii).- Por (ii), $\mathbb{K} = \mathbb{F}(\delta)$ para algún $\delta^2 = D \in \mathbb{F} \setminus \{0\}$. Luego, $\{1, \delta\}$ es base de $\mathbb{K}$ como espacio vectorial sobre $\mathbb{F}$. Sigue que para $\omega \in \mathbb{K}$ existen ω_0 y ω_1 en $\mathbb{F}$ tales que $\omega = \omega_0 + \omega_1\delta$. Del punto anterior tenemos que $\omega^2 \in \mathbb{F}$ si y sólo si $\varphi(\omega^2) = \omega^2$ para todo $\varphi \in \mathbf{Gal}(\mathbb{K}|_{\mathbb{F}}) = \{id, \sigma\}$ donde $\sigma(\delta) = -\delta$. Luego, $\omega^2 \in \mathbb{F}$ si y sólo si $\sigma(\omega^2) = \omega^2$, i.e.,

$$\omega_0^2 - \omega_1^2 D + 2\omega_0\omega_1\delta = \omega_0^2 - \omega_1^2 D - 2\omega_0\omega_1\delta\,.$$

En otras palabras, $\omega_0 = 0$ o $\omega_1 = 0$. Resumiendo,

$$\big\{\omega \in \mathbb{K} \,:\, \omega^2 \in \mathbb{F}\big\} = \mathbb{F} \cup \delta\mathbb{F}\,.$$