Prueba 1, Cuerpos y Álgebras, 25 de octubre de 2018.

Resuelva al menos tres de los siguientes problemas.

1. Determine el cuerpo de descomposición de $x^5 - 5 \in \mathbb{Q}[x]$ y calcule su grado.

   Solución: Observemos en primer lugar que $x^5 - 5$ es un polinomio irreducible por el criterio de Eisenstein aplicado con el primo 5. Las raíces en $\mathbb{C}$ del polinomio $x^5 - 5$ son $\{\sqrt[5]{5}, \zeta_5\sqrt[5]{5}, \zeta_5^2\sqrt[5]{5}, \zeta_5^3\sqrt[5]{5}, \zeta_5^4\sqrt[5]{5}\}$ Es fácil ver que el cuerpo generado por estas raíces es $L = \mathbb{Q}[\zeta_5, \sqrt[5]{5}]$ por lo que L es el cuerpo de descomposición buscado. Para determinar su grado, consideremos primero las extensiones simples sobre $\mathbb{Q}$ generadas por ζ_5 y $\sqrt[5]{5}$ respectivamente. Los grados de estas extensiones son 4 y 5 respectivamente. Como L contiene a ambas subextensiones, tenemos que tanto 4 como 5 dividen a $|L : \mathbb{Q}|$. Además es claro que, por ser L el composito de ambas, $|L : \mathbb{Q}| \leq 20$. Concluimos que $|L : \mathbb{Q}| = 20$.

2. Sea $\Phi_n(x)$ el polinomio ciclotómico de orden n y μ la función de Möbius. Demuestre que

$$\Phi_n(x) = \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}$$

   Ayuda: Puede usar que

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$

   Solución: Supondremos conocido que para todo $n \in \mathbb{N}$,

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

   Procedemos a calcular

$$\begin{aligned}
\prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)} &= \prod_{d|n} \left(\prod_{e|\frac{n}{d}} \Phi_e(x) \right)^{\mu(d)} && (1) \\
&= \prod_{d|n} \prod_{e|\frac{n}{d}} (\Phi_e(x))^{\mu(d)} && (2) \\
&= \prod_{e|n} \prod_{d|\frac{n}{e}} (\Phi_e(x))^{\mu(d)} && (3) \\
&= \prod_{e|n} (\Phi_e(x))^{\sum_{d|\frac{n}{e}} \mu(d)} && (4) \\
&= \Phi_n(x) && (5)
\end{aligned}$$

   El paso 3 se justifica notando que

$$\{(d, e) : d \mid n \wedge e \mid \frac{n}{d}\} = \{(d, e) : (de) \mid n\} = \{(d, e) : e \mid n \wedge d \mid \frac{n}{e}\}$$

   El último paso se obtiene usando la sugerencia pues de ahí se desprende que el exponente es 0 salvo cuando $e = n$ y en ese caso es 1.

3. Sea K una extensión finita de F. Demuestre que K es un cuerpo de descomposición sobre F si y solo si todo polinomio irreducible en $F[x]$ que tiene una raíz en K se descompone completamente en $K[x]$.

   Solución: Supongamos primero que K es un cuerpo de descomposición sobre F y para fijar notación, digamos que $K = F(\gamma_1, \ldots, \gamma_n)$ con $\{\gamma_1, \ldots, \gamma_n\}$ el conjunto de todas las raíces de un polinomio $p(x) \in F[x]$. Supongamos ahora que $f(x) \in F[x]$ es un polinomio irreducible que tiene una raíz $\alpha \in K$. Si $\beta \in \overline{K}$ es otra raíz de f, sabemos que existe un isomorfismo $\varphi : F[\alpha] \to F[\beta]$ que restringido a F es la identidad y que cumple que $\varphi(\alpha) = \beta$. Falta que demostremos que $\varphi(\alpha) \in K$. Para ello notemos que $\varphi(\gamma_i) \in \{\gamma_1, \ldots, \gamma_n\}$ para todo γ_i pues al fijar los coeficientes de $p(x)$, φ debe enviar una raíz de p en otra raíz de p. Podemos concluir que $\varphi(K) = K$ y por lo tanto $\varphi(\alpha) \in K$. Finalmente, al ser β una raíz arbitraria de f, tenemos que f se descomopone completamente en $K[x]$.

   Ahora supongamos que todo polinomio $f(x) \in F[x]$ que tiene una raíz en K se descompone completamente. Como K/F es una extensión finita, sabemos que existen $\{\alpha_1, \ldots, \alpha_t\}$ tales que $K = F[\alpha_1, \ldots, \alpha_t]$. Consideremos los polinomios minimales $p_i(x)$ para cada uno de los α_i y definamos $p(x)$ como el producto de todos ellos. Como cada $p_i(x)$ tiene al menos una raíz en K, podemos usar la hipótesis para concluir que cada $p_i(x)$ se factoriza completamente en $K[x]$ y por lo tanto que $p(x)$ se factoriza completamente en $K[x]$. Por otra parte, K está generado, sobre F, por algunas de las raíces de $p(x)$ de manera que está contenido en el cuerpo de descomposiciónde $p(x)$ sobre F. Concluimos que K es el cuerpo de descomposición de $p(x)$ sobre F.

4. Sea $L = \mathbb{F}_p(x, y)$ y $K = \mathbb{F}_p(x^p, y^p)$. Demuestre que L/K es una extensión puramente inseparable de grado p^2 y que no existe $\alpha \in L$ tal que $L = K[\alpha]$.

   Solución: Como x^p es primo en $\mathbb{F}_p[x^p, y^p]$ (anillo de polinomios en dos variables) y K es su cuerpo de fracciones, podemos usar el criterio de Eisenstein para decir que $t^p - x^p \in K[t]$ es irreducible. De forma similar, $t^p - y^p$ es irreducible en $K(x)[t]$. Como $L = K(x, y)$ podemos calcular el grado de la extensión

$$|K(x, y) : K| = |K(x)(y) : K(x)||K(x) : K| = p^2$$

   Ahora consideremos un elemento arbitrario $a \in L$. Escribimos $a = \frac{f(x,y)}{g(x,y)}$ con f y g polinomios en $\mathbb{F}_p[x, y]$. Entonces a es raíz del polinomio $t^p - a^p = t^p - \frac{f(x^p,y^p)}{g(x^p,y^p) \in K[t]}$. En particular $|K(a) : K| \leq p$ por lo que no se puede tener $L = K(a)$.

   Por otra parte, en $L[t]$ el polinomio $t^p - a^p$ se factoriza como $t^p - a^p = (t - a)^p$. Si suponemos que a es separable sobre K, entonces el polinomio minimal de a sobre K no tiene raíces repetidas, por lo que es $t - a$ y $a \in K$. Esto comprueba que la extensión es puramente inseparable.