Prueba 1, Algebra II, 12 de septiembre de 2018.

Elija y resuelva tres de los siguientes ejercicios.

1. Sea L/K una extensión de Galois y sean M, M' subcuerpos de L que contienen a K . Sean $H = \text{Gal}(L/M)$ y $H' = \text{Gal}(L/M')$. Demuestre que $\text{Gal}(L/MM') = H \cap H'$ y $L^{H \cap H'} = MM'$.

Solución: Como $H \cap H' \subseteq H$ podemos usar el teorema fundamental para decir que $M \subseteq L^{H \cap H'}$. De forma similar, $M' \subseteq L^{H \cap H'}$. Como MM' es el menor cuerpo que contiene a M y M' , concluimos que $MM' \subseteq L^{H \cap H'}$.

Para demostrar la contención que falta, volvemos a usar el teorema fundamental, ahora considerando que $M \subseteq MM'$ por lo que $\text{Gal}(L/MM') \subseteq H$ y similarmente $\text{Gal}(L/MM') \subseteq H'$ por lo que $\text{Gal}(L/MM') \subseteq H \cap H'$. Usando el mismo teorema, $L^{H \cap H'} \subseteq MM'$. Concluimos que $MM' = L^{H \cap H'}$ y por lo tanto que también $\text{Gal}(L/MM') = H \cap H'$.

2. Considere el cuerpo finito $\mathbb{F}_5$

- (a) ¿Cuántos polinomios irreducibles mónicos de grado 6 hay en $\mathbb{F}_5[x]$?

Solución: Sabemos que cualquier polinomio irreducible de grado 6 tiene todas sus raíces en $\mathbb{F}_{5^6}$ y que todo elemento en $\mathbb{F}_{5^6}$ que no está en un subcuerpo propio es raíz de un polinomio irreducible de grado 6 en $\mathbb{F}_5[x]$. Para contar estos elementos usamos el principio de inclusión/exclusión. Los subcuerpos de $\mathbb{F}_{5^6}$ son $\mathbb{F}_5, \mathbb{F}_{5^2}$ y $\mathbb{F}_{5^3}$. Finalmente, como cada uno de los polinomios buscados tiene 6 raíces diferentes, dividimos el resultado por 6 para obtener el número de polinomios.

$$N = \frac{5^6 - 5^3 - 5^2 + 5}{6} = 2580$$

- (b) Determine el grupo de Galois del cuerpo de descomposición de $x^6 - 1$ sobre $\mathbb{F}_5$.

Solución: Primero debemos factorizar completamente $x^6 - 1$ sobre $\mathbb{F}_5$. Afortunadamente ya lo podemos factorizar significativamente en $\mathbb{Z}[x]$:

$$x^6 - 1 = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$$

Ahora solo falta verificar que los factores cuadráticos no tienen raíces en $\mathbb{F}_5$ por lo que son irreducibles. Esto es un cálculo sencillo que dejamos al lector.

De esto concluimos que el cuerpo de descomposición es $\mathbb{F}_{25}$. Como se trata de una extensión de grado 2, su grupo de Galois es cíclico de orden 2.

3. Determine el cuerpo de descomposición K para el polinomio $p(x) = x^7 - 7$ sobre $\mathbb{Q}$. Describa el grupo $\text{Gal}(K/\mathbb{Q})$ en términos de generadores y relaciones. Muestre como actúan los generadores del grupo en K .

Solución: Por el criterio de Eisenstein, el polinomio dado es irreducible por lo que una raíz genera una extensión de grado 7. Para completar el cuerpo de descomposición debemos agregar una raíz séptima de la unidad. Como el polinomio minimal de la raíz séptima es de grado 6, relativamente primo a 7, el compuesto de las dos extensiones de $\mathbb{Q}$ es una extensión de grado 42. Definamos $K = \mathbb{Q}[\sqrt[7]{7}, \zeta_7]$ y $G = \text{Gal}(K/\mathbb{Q})$. Debiera ser

claro que K es el cuerpo de descomposición buscado. Como $\mathbb{Q}[\zeta_7]/\mathbb{Q}$ es una extensión galoisiana, Sabemos que $N = \text{Gal}(K/Q[\zeta_7])$ es un subgrupo normal de G de orden 7 (también podríamos usar teoremas de Sylow para esto). Definamos un generador de N como $\sigma : K \rightarrow K$ de manera que $\sigma(\sqrt[7]{7}) = \zeta_7 \sqrt[7]{7}$. Para el subgrupo $H = \text{Gal}(K/Q[\sqrt[7]{7}])$ definimos un generador $\tau : K \rightarrow K$ de manera que $\tau(\zeta_7) = \zeta_7^3$. Acá la elección de exponente debe ser cuidadosa para asegurar que τ sea efectivamente un generador del grupo cíclico de orden 6. Así tenemos que $G = \langle \sigma, \tau \rangle$ y solo nos falta determinar como actúa τ en N .

$$\tau\sigma\tau^{-1}(\sqrt[7]{7}) = \tau(\zeta_7 \sqrt[7]{7}) = \zeta_7^3 \sqrt[7]{7},$$

es decir $\tau\sigma\tau^{-1} = \sigma^3$. La presentación pedida es

$$G \cong \langle s, t \mid s^7 = t^6 = 1, sts^{-1} = s^3 \rangle.$$

4. Sea F un cuerpo de característica p y $\alpha \in \overline{F}$ un elemento separable. Muestre que $F(\alpha) = F(\alpha^{p^i})$, para todo $i \in \mathbb{N}$.

Solución: Como es claro que $F(\alpha^{p^i}) \subseteq F(\alpha)$, basta con demostrar que la extensión $F(\alpha)/F(\alpha^{p^i})$ es de grado 1. Sea $f(x)$ el polinomio minimal de α sobre $F(\alpha^{p^i})$. Como α es raíz del polinomio $r(x) = x^{p^i} - \alpha^{p^i} \in F(\alpha^{p^i})[x]$, sabemos que $f(x)$ divide a $r(x)$. Notemos que $r(x) = (x - \alpha)^{p^i}$ y que como α es separable, todas las raíces de $f(x)$ en $F(\alpha)$ son diferentes. De esto concluimos que $f(x) = x - \alpha$ y la extensión es de grado 1 como queríamos demostrar.