Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y Teoría de Galois
Primer semestre de 2020

Práctico 9

1. Probar que si K es un cuerpo finito, entonces $\mathrm{car}(K) = p > 0$ y existe $n \in \mathbb{Z}^+$ tal que $|K| = p^n$.

2. *a*) Probar que el polinomio $f = X^3 - 6X^2 + 9X + 3$ es irreducible sobre $\mathbb{Q}$.
   b) Se considera la extensión $\mathbb{Q}(u) \supset \mathbb{Q}$ donde u es una raíz real de f. Expresar u^4 y $(u+1)^{-1}$ como combinación lineal de los elementos de la base $\{1, u, u^2\}$

3. Se consideran el polinomio $f = X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$ y la extensión $\mathbb{Q}\left(\sqrt{2}, i\right) / \mathbb{Q}$.
   a) Calcular $\left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\right]$ y hallar una base de $\mathbb{Q}\left(\sqrt{2}, i\right)$ como $\mathbb{Q}$-espacio.
   Sugerencia: considerar $\mathbb{Q}\left(\sqrt{2}, i\right) \supset \mathbb{Q}\left(\sqrt{2}\right) \supset \mathbb{Q}$.
   b) Observar que $f = \left(X^2 - 3\right)^2 + 4X^2$ y deducir que el polinomio f escinde en $\mathbb{Q}\left(\sqrt{2}, i\right)$.
   c) Probar que f es irreducible sobre $\mathbb{Q}$.
   d) Probar que $\mathbb{Q}\left(\sqrt{2}, i\right) = \mathbb{Q}(u)$, siendo $u = \sqrt{2} + i$.
   e) Hallar $\mathrm{Irr}_{\mathbb{Q}\left(\sqrt{2}\right)}(u)$, $\mathrm{Irr}_{\mathbb{Q}\left(\sqrt{3}\right)}(u)$, $\mathrm{Irr}_{\mathbb{Q}(i)}(u)$ y $\mathrm{Irr}_{\mathbb{Q}\left(i\sqrt{2}\right)}(u)$.

4. Sea F/K una extensión algebraica y $A \subset F$ un subanillo tal que $K \subset A$. Probar que A es un cuerpo.

5. Sean $u, v \in F \supset K$ algebraicos sobre K de grados m y n. Probar que si $\mathrm{mcd}(m, n) = 1$, entonces $[K(u, v) : K] = mn$.

6. Probar que $u = \sqrt{2} + \sqrt[3]{5}$ es algebraico sobre $\mathbb{Q}$ de grado 6. ¿Cuál es el grado de u sobre $\mathbb{Q}(\sqrt{2})$ y sobre $\mathbb{Q}(\sqrt[3]{5})$? Hallar los polinomios irreducibles de u sobre $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{5})$.

7. Hallar una base de F sobre $\mathbb{Q}$, donde $F = \mathbb{Q}\left(i, \sqrt{3}, \omega\right)$, siendo $\omega \neq 1$ una raíz cúbica de 1.

8. Hallar $u \in \mathbb{R}$ tal que $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right) = \mathbb{Q}(u)$, siendo p y q primos distintos.

9. Sea F/K una extensión.
   a) Si $u \in F$ es algebraico de grado impar sobre K, probar que $K(u) = K\left(u^2\right)$.
   b) Sean $f = X^n - a \in K[X]$ irreducible, $u \in F$ una raíz de f y m un divisor de n. Probar que el grado de u^m sobre K es n/m. ¿Cuál es el polinomio irreducible de u sobre $K(u^m)$?

10. Sea K, E, L subcuerpos de un cuerpo F tales que $K \subset E$ y $K \subset L$. Probar.
    a) Si $u \in F$ es algebraico sobre K, entonces u es algebraico sobre L y $[L(u) : L] \leq [K(u) : K]$.
    b) Si $u_1, \ldots, u_n \in F$ son algebraicos sobre K, entonces
    $$[L(u_1, \ldots, u_n) : L(u_1, \ldots, u_{n-1})] \leq [K(u_1, \ldots, u_n) : K(u_1, \ldots, u_{n-1})].$$
    c) Si E/K es finita, entonces EL/L es finita y $[EL : L] \leq [E : K]$.
    d) Si E/K y L/K son finitas, entonces $[EL : K] \leq [E : K][L : K]$. Si además se cumple $\mathrm{mcd}\left([E : K], [L : K]\right) = 1$, entonces $[EL : K] = [E : K][L : K]$.