Guía de Ejercicios y tarea 1.
Cuerpos y Álgebras, segundo semestre 2018

Entregue resueltos los 2 ejercicios marcados con * el jueves 4 de octubre.

1. Encuentre el polinomio minimal de $\sqrt{2} + \sqrt[3]{2}$ en $\mathbb{Q}[x]$.

2. *Determine los elementos primitivos de $\mathbb{F}_{19}$.

3. Determine los elementos primitivos de $\mathbb{F}_{49} = \mathbb{F}_7[i]$ y sus polinomios minimales en $\mathbb{F}_7[x]$. (Acá i denota una raíz de $x^2 + 1 \in \mathbb{F}_7[x]$)

4. Suponga que $\operatorname{car}(F) = p \neq 0$. Demuestre que el morfismo de Frobenius $x \mapsto x^p$ es un automorfismo de cuerpos de F. Si pensamos en F como $\mathbb{F}_p$-espacio vectorial, ¿es $\mathbb{F}_p$-lineal este morfismo?

5. Si F es un cuerpo de característica $p > 0$ y $\alpha \in F$ ¿cuántas soluciones diferentes puede tener (en alguna extensión de F) la ecuación $x^p = \alpha$? ¿Y la ecuación $x^{p^k} = \alpha$ con $k \in \mathbb{N}$?

6. Si $\mathbb{F}$ es un cuerpo finito de característica p y $\alpha \in \mathbb{F}$, ¿puede $X^p - \alpha$ ser irreducible en $\mathbb{F}[X]$?

7. * Sea $n \in \mathbb{N}$, sea $\mathbb{F}_p$ el cuerpo finito de p elementos con p primo, y sea L un cuerpo de descomposición del polinomio $G(X) := X^{p^n} - X \in \mathbb{F}_p[X]$.

   a) Demuestre que $G(X)$ es un polinomio separable, pero NO irreducible en $\mathbb{F}_p[X]$.

   b) Demuestre que el conjunto de las raíces de G es un subcuerpo de L.

   c) Demuestre que L es igual al conjunto de raíces de G.

   d) Demuestre que $[L : \mathbb{F}_p] = n$.

   e) Demuestre que toda extensión de $K/\,\mathbb{F}_p$ de grado n es isomorfa a L.

8. Sea $\mathbb{F}_q$ el cuerpo finito de q elementos, de modo que $q = p^n$ para algún primo p y algún $n \in \mathbb{N}$. ¿Cuando se cumple que hay una inyección $\mathbb{F}_q \to \mathbb{F}_{q'}$?

9. Sea p primo y $a \neq 0 \in \mathbb{F}_p$. Demuestre que $g = x^p - x + a$ es irreducible y separable sobre $\mathbb{F}_p$. Determine el cuerpo de descomposición de g sobre $\mathbb{F}_p$. Muestre explícitamente que su grupo de automorfismos es cíclico. ($\alpha \mapsto \alpha + 1$ define un automorfismo)

10. Calcule el grupo de automorfismos del cuerpo $\mathbb{F}_q$.

Guía de Ejercicios y tarea 2.
Cuerpos y Álgebras, segundo semestre 2018

Entregar los 3 ejercicios marcados el jueves 18 de octubre.

1. Demuestre que $x^{p^n} - x + 1$ es irreducible sobre $\mathbb{F}_p$ solo si $n = 1$ o $n = p = 2$. Ayuda: Si α es una raíz, entonces $\alpha + a$ también es raíz para todo $a \in \mathbb{F}_{p^n}$. Muestre que esto implica que $\mathbb{F}_p(\alpha)$ contiene $\mathbb{F}_{p^n}$ y $[\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}] = p$.

2. ¿Cuántos factores irreducibles sobre $\mathbb{F}_3[X]$ tiene el polinomio $X^{27} - X$?

3. Un cuerpo de característica p se dice perfecto si la función $\alpha \mapsto \alpha^p$ es sobreyectiva.

   a) Demuestre que todo cuerpo finito es perfecto.

   b) Demuestre que Si F es un cuerpo cualquiera de característica p, entonces $F(x)$ no es perfecto.

4. Sea $F = \mathbb{F}_p(T)$ el cuerpo de funciones racionales sobre un cuerpo primo finito y sea K/F el cuerpo de descomposición del polinomio $X^p - T$. Demuestre que $[K : F] = p$ y que hay un único F-automorfismo del cuerpo K.

5. Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible de grado k. Demuestre que f divide a $x^{q^n} - x$ si y solo si k divide a n.

6. Demuestre que
$$\sum_{a \in F_q} a^t = \begin{cases} 0 & \text{si } 1 \leq t \leq q-2 \\ -1 & \text{si } t = q-1 \end{cases}$$

7. Demuestre que $X^3 - 2X - 2$ es irreducible sobre $\mathbb{Q}$. Si θ es una raíz de este polinomio, calcule $(1+\theta)(1+\theta+\theta^2)$ y $\frac{1+\theta}{1+\theta+\theta^2}$ en $\mathbb{Q}(\theta)$.

8. Sea K/F una extensión de cuerpos. Si $u \in K$ es un elemento algebraico de grado impar sobre F, entonces u^2 también lo es y $F[u] = F[u^2]$.

9. * En el cuerpo de funciones racionales $F(X)$, sea $u = \frac{X^3}{X+1}$. Demuestre que $F(X)$ es una extensión simple de $F(u)$. Calcule $[F(X) : F(u)]$.

10. Determine el cuerpo de descomposición y su grado sobre $\mathbb{Q}$ para cada uno de los polinomios siguientes:

    a) $x^4 - 2$ *b*) $x^4 + 2$ *c*) $x^4 + x^2 + 1$

11. Sea $f(x) \in F[x]$ un polinomio irreducible de grado p y sea $E \supseteq F$ con $|E : F| < \infty$. Si $f(x)$ no es irreducible en $E[x]$, demuestre que $p \mid |E : F|$. Ayuda: Considere un cuerpo $L \supseteq E$ en el que f tenga una raíz.

12. 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 $K[x]$.

13. * Sean K_1, K_2 extensiones finitas de F contenidas en K y suponga que ambas son cuerpos de descomposición sobre F. Demuestre que el composito K_1K_2 y la intersección $K_1 \cap K_2$ son cuerpos de descomposición sobre F.

14. * Sea $\overline{\mathbb{Q}} \subset \mathbb{C}$ la clausura algebraica de $\mathbb{Q}$ en $\mathbb{C}$.

    a) Demuestre que $\overline{\mathbb{Q}}$ es denumerable.

    b) Demuestre que $\overline{\mathbb{Q}}/\mathbb{Q}$ es una extensión algebraica infinita.

    c) Sea $\alpha \in \overline{\mathbb{Q}} \cap \mathbb{R}$ y $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Demuestre que el conjunto de racionales p/q (con $p, q \in \mathbb{Z}$) tales que $|\alpha - p/q| < 1/q^{n+1}$ es finito (o vacío). Concluya (como Liouville alrededor de 1829) que $\sum_{j=0}^{\infty} 10^{-j!}$ es un número real no algebraico.

       SUGERENCIA. Sea $P(X) \in \mathbb{Z}(X)$ de grado n y tal que $P(\alpha) = 0$. Considere $|P(p/q)| = |P(p/q) - P(\alpha)|$ y piense en el teorema del valor medio.

15. Sea F, un cuerpo y $g(x) \in F[x]$. Demuestre $D(g(x))$ es el polinomio nulo ssi $g(x)$ es constante, o F es de característica p y $g(x) = f(x^p)$, con $f(x) \in F[x]$.

16. Demuestre que el único automorfismo del cuerpo $\mathbb{R}$ es la identidad.

17. Demuestre que la clausura algebraica $\overline{\mathbb{Q}}$ tiene infinitos automorfismos. Más aún, demuestre que el grupo de automorfismos (de cuerpo) de $\overline{\mathbb{Q}}$ no es denumerable.

18. Sea $f(x)$ un polinomio irreducible en $F[x]$ de grado n y sea $g(x) \in F[x]$. Muestre que todo factor irreducible de $f(g(x))$ tiene grado divisible por n.

19. Sea $K \subset L$ cuerpos y $a \in L$. Pruebe que a es algebraico sobre K si y solamente si existe un K-espacio vectorial de dimensión finita $V \subset L$ tal que $aV \subset V$.

20. Sea w una raiz cúbica y no trivial de la unidad. Sea $L = \mathbb{Q}(w, \sqrt[3]{2})$ y $K = \mathbb{Q}(w\sqrt[3]{2})$. Pruebe que $[L : K] = 2$, pero $[L \cap \mathbb{R} : K \cap \mathbb{R}] = 3$.

21. Demuestre que el cuerpo de descomposición de $x^4 + 2$ sobre $\mathbb{F}_5$ es una extensión de grado 2 de $\mathbb{F}_5$.

22. Suponga que K es un cuerpo de característica p que no es perfecto. Pruebe que existe un polinomio irreducible e inseparable sobre K. Concluya que existe una extensión inseparable de K.