

Guía de Ejercicios y tarea 1.
Álgebra II, segundo semestre 2018

Entregue resueltos los 4 ejercicios marcados con * el miércoles 8 de agosto.

1. Determine los elementos primitivos de $\mathbb{F}_7$.
2. * 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 $x^2 + 1 \in \mathbb{F}_7[x]$)
3. Suponga que $\text{car}(F) = p \neq 0$. 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?
4. Si F es un cuerpo de característica $p > 0$ y $\alpha \in F$ ¿cuántas soluciones puede tener (en alguna extensión de F) la ecuación $x^p = \alpha$? ¿Y la ecuación $x^{p^k} = \alpha$ con $k \in \mathbb{N}$?
5. Si $\mathbb{F}$ es un cuerpo finito de característica p y $\alpha \in \mathbb{F}$, ¿puede $X^p - \alpha$ ser irreducible en $\mathbb{F}[X]$?
6. 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 .
7. Sea $\mathbb{F}_q$ el cuerpo finito de q elementos, de modo que $q = p^n$ para algún primo p y algún $n \in \mathbb{N}$. ¿Cuándo se cumple que hay una inyección $\mathbb{F}_q \rightarrow \mathbb{F}_{q'}$?
8. * 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)
9. Calcule el grupo de automorfismos del cuerpo $\mathbb{F}_q$.
10. 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 $[\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}] = p$.

11. ¿Cuántos factores irreducibles sobre $\mathbb{F}_3[X]$ tiene el polinomio $X^{27} - X$?
12. 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.
13. 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 .
14. 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 .
15. Demuestre que

$$\sum_{a \in \mathbb{F}_q} a^t = \begin{cases} 0 & \text{si } 1 \leq t \leq q-2 \\ -1 & \text{si } t = q-1 \end{cases}$$
16. 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 $\mathbb{Q}(\theta)$.
17. * Encuentre los valores de $a \in \mathbb{Z}$ tales que $X^5 - aX - 1$ sea irreducible en $\mathbb{Z}[X]$.
18. 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 $F[u] = F[u^2]$.
19. 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 $[F(X) : F(u)]$.
20. * Sea K/F una extensión de cuerpos, sean L/F y M/F subextensiones finitas de K/F (es decir, $F \subset L \subset K$, $F \subset M \subset K$, $[L : F] < \infty$, $[M : F] < \infty$). Sea LM el compósito de L y M dentro de K (es decir, el mínimo subcuerpo de K que contiene a L y a M).
 - a) Demuestre que $[LM : F] < \infty$, y que $[L : F] \mid [LM : F]$.
 - b) Demuestre que $[LM : F] = [L : F][M : F]$ implica $L \cap M = F$.
 - c) Demuestre que el recíproco se verifica cuando $[L : F] = 2$ o $[M : F] = 2$.
 - d) Dé un ejemplo de extensiones F, L, M, K tal que $[L : F] = [M : F] = 3$, $[LM : F] < 9$, $L \cap M = F$.
21. 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.

Guía de Ejercicios y tarea 2.
Álgebra II, segundo semestre 2018

Entregar los 4 ejercicios marcados el lunes 27 de agosto.

1. 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) $x^4 + x^2 + 1$

2. * 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 $K[x]$.
3. * 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 $K_1 K_2$ y la intersección $K_1 \cap K_2$ son cuerpos de descomposición sobre F .
4. 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.

5. 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 $f(x) \in F[x]$.
6. Demuestre que el único automorfismo del cuerpo $\mathbb{R}$ es la identidad.
7. 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.
8. 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 .
9. 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 $aV \subset V$.
10. Sea w una raíz 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 $[L \cap \mathbb{R} : K \cap \mathbb{R}] = 3$.

11. Demuestre que el cuerpo de descomposición de $x^4 + 2$ sobre $\mathbb{F}_5$ es una extensión de grado 2 de $\mathbb{F}_5$.
12. * 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 .
13. Sea F un cuerpo de característica p y F/K una extensión finita tal que $p \nmid [F : K]$. Pruebe que F/K es una extensión separable.
14. 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 $i \in \mathbb{N}$.
15. Sea K/F una extensión separable con la propiedad que existe $n \in \mathbb{N}$ tal que $[F(\alpha) : F] \leq n$, para todo $\alpha \in K$. Muestre que K/F es finita y que $[K : F] \leq n$.
16. Sea K el cuerpo de descomposición del polinomio $p(x) = (x^2 - 2)(x^4 + x^2 + 2)$ en $\mathbb{F}_5$. Encuentre un elemento primitivo para la extensión $K/\mathbb{F}_5$.
17. Encuentre todos los polinomios irreducibles de grado 1, 2 y 4 sobre $\mathbb{F}_2[x]$ y pruebe que su producto es $x^{16} - x$.
18. Sea $\mathbb{F}_{p^n} = \{\alpha_1, \dots, \alpha_{p^n}\}$ la extensión de grado n de $\mathbb{F}_p$. Pruebe que $x^{p^n} - x = (x - \alpha_1) \cdots (x - \alpha_{p^n})$.
19. Sea $\mathbb{F}_{p^n}$ la extensión de grado n de $\mathbb{F}_p$. Pruebe que en $\mathbb{F}_{p^n}$ hay $\frac{p^n+1}{2}$ cuadrados.
20. * Demuestre que en un cuerpo finito todo elemento es suma de dos cuadrados.
21. Sea $\phi : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ el homomorfismo de Frobenius. Pruebe que $\phi^n = \text{id}$ y que $\phi^s \neq \text{id}$, para $0 < s < n$.
22. Sea L/F una extensión algebraica y sea $\theta : L \rightarrow L$ un F -homomorfismo de cuerpos. Demuestre que θ es sobreyectivo. Ayuda: Un polinomio $f \in F[x]$ debe tener tantas raíces en $\theta(L)$ como tiene en L .