Guía de Ejercicios y tarea 1.
Álgebra II, segundo semestre 2013

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 $\mathrm{car}(F) = p \neq 0$. 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 $n \in \mathbb{N}$. ¿Cuando se cumple que hay una inyección $\mathbb{F}_q \to \mathbb{F}_{q'}$?
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

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

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 $[L : F] \big| [LM : F]$.

    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.