Álgebra II. Hoja de ejercicios 11: Cuerpos finitos II
Universidad de El Salvador, ciclo par 2018

Por cualquier pregunta, no duden en escribir al grupo ues-algebra-2@googlegroups.com.

Ejercicio 1. *Sea $q = p^k$ donde p es primo y $k = 1, 2, 3, \ldots$ Demuestre que para cualquier $n = 1, 2, 3, \ldots$ existe un polinomio mónico irreducible $f \in \mathbb{F}_q[X]$ de grado n. (Lo probamos en clase para $k = 1$.)*

Ejercicio 2. *Encuentre isomorfismos explícitos entre los cuerpos*

$$\mathbb{F}_3[X]/(X^2+1), \quad \mathbb{F}_3[X]/(X^2+X+2), \quad \mathbb{F}_3[X]/(X^2+2X+2).$$

Ejercicio 3. *Encuentre los polinomios mónicos irreducibles de grado 3 en $\mathbb{F}_2[X]$ factorizando $X^8 - X$.*

Ejercicio 4. *Sean p y q dos diferentes primos impares. Demuestre que el número de polinomios mónicos irreducibles de grado q en $\mathbb{F}_p[X]$ es igual a $\frac{1}{q}(p^q - p)$.*

Ejercicio 5. *Sea k un cuerpo.*

1) *Demuestre que los cuadrados en el grupo multiplicativo $k^\times$ forman un subgrupo*

$$(k^\times)^2 := \{\alpha \in k^\times \mid \alpha = x^2 \text{ para algún } x \in k^\times\} \subseteq k^\times.$$

2) *Enumere los cuadrados en el grupo $\mathbb{F}_9^\times$ para el cuerpo $\mathbb{F}_9$ construido en la guía anterior.*

3) *Calcule el grupo cociente $k^\times/(k^\times)^2$ para $k = \mathbb{R}$ y $k = \mathbb{F}_q$, donde $q = p^k$ (considere por separado el caso de $p = 2$ y p impar).*

Ejercicio 6. *Sea $q = p^k$ donde p es un primo impar y $k = 1, 2, 3, \ldots$ Demuestre que -1 es un cuadrado en $\mathbb{F}_q$ si y solamente si -1 tiene orden 4 en el grupo cíclico $\mathbb{F}_q^\times$. Concluya que -1 es un cuadrado en $\mathbb{F}_q$ si y solamente si $q \equiv 1 \pmod 4$.*

Ejercicio 7 (generalización de 5)**.** *Sea $q = p^k$ donde p es primo y $k = 1, 2, 3, \ldots$ Asumamos que $q \equiv 1 \pmod n$.*

1) *Demuestre que para todo $\alpha \in \mathbb{F}_q^\times$ la ecuación $x^n = \alpha$ o no tiene soluciones, o tiene n soluciones.*

2) *Demuestre que el subconjunto*

$$\{\alpha \in \mathbb{F}_q^\times \mid \alpha = x^n \text{ para algún } x \in \mathbb{F}_q^\times\}$$

es un subgrupo de $\mathbb{F}_q^\times$ de orden $\frac{q-1}{n}$.

3) *Por ejemplo, encuentre el subgrupo de cubos en $\mathbb{F}_{13}^\times$.*

Ejercicio 8. *Supongamos que p es un primo tal que $p \equiv 3 \pmod 4$. Demuestre que el anillo cociente $\mathbb{Z}[\sqrt{-1}]/(p)$ es un cuerpo de p^2 elementos.*