Universidad de El Salvador. 6.12.2018
Álgebra II. Examen parcial 2

Problema 1 (2 puntos)**.** Para el polinomio $f := X^3 + 3X + 2 \in \mathbb{Q}[X]$, sean K el anillo cociente $\mathbb{Q}[X]/(f)$ y $\alpha \in K$ la imagen de X en el cociente.

a) Demuestre que K es un cuerpo. [$\frac{1}{2}$ *punto*]

b) Exprese α^{-1} en la base $1, \alpha, \alpha^2$. [$\frac{1}{2}$ *punto*]

c) ¿Es cierto o falso que existe $\beta \in K$ tal que $\beta^3 = \alpha$? [1 *punto*]

Problema 2 (2 puntos)**.** Sean p un número primo y $n = 1, 2, 3, \ldots$ Para el cuerpo finito $\mathbb{F}_{p^n}$ y un elemento $\alpha \in \mathbb{F}_{p^n}$ definamos $t(\alpha) := \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$.

a) Demuestre que $t(\alpha) \in \mathbb{F}_p$. [1 *punto*]

b) Demuestre que $t\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ es una aplicación $\mathbb{F}_p$-lineal. [$\frac{1}{2}$ *punto*]

c) Demuestre que la aplicación $t\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ es sobreyectiva. [$\frac{1}{2}$ *punto*]

Problema 3 (2 puntos)**.** Sea p un número primo. Consideremos el polinomio $f := X^2 + X + 1 \in \mathbb{F}_p[X]$.

a) Demuestre que f es irreducible si y solo si $p \equiv 2 \pmod{3}$. [1 *punto*]

b) ¿Para cuáles p el polinomio f es separable? [1 *punto*]

Problema 4 (2 puntos)**.** Sean p un primo impar y n un número natural tal que $p \nmid n$. Denotemos por $\Phi_n \in \mathbb{Z}[X]$ el n-ésimo polinomio ciclotómico.

a) Demuestre que el polinomio $X^n - 1 \in \mathbb{F}_p[X]$ es separable. [1 *punto*]

b) Demuestre que si $a \in \mathbb{Z}$ satisface $\Phi_n(a) \equiv 0 \pmod{p}$, entonces $p \nmid a$ y el orden de a en $(\mathbb{Z}/p\mathbb{Z})^\times$ es igual a n. [1 *punto*]

Indicación: factorice $X^n - 1 \in \mathbb{Z}[X]$ en polinomios ciclotómicos.

Problema 5 (2 puntos)**.** Sean p un número primo y $a \in \mathbb{F}_p$ un elemento no nulo. Consideremos el polinomio $f := X^p - X + a \in \mathbb{F}_p[X]$. En este problema vamos a probar que f es irreducible.

a) Demuestre que f es separable. [$\frac{1}{2}$ *punto*]

b) Sea L un cuerpo de descomposición de f y sea $\alpha \in L$ un elemento tal que $f(\alpha) = 0$. Demuestre que las raíces de f en L son $\alpha, \alpha + 1, \ldots, \alpha + p - 1$. [$\frac{1}{2}$ *punto*]

c) Asumamos que $f = gh$ donde $g, h \in \mathbb{F}_p[X]$ son polinomios mónicos y $\deg g, \deg h < \deg f$. Analizando la suma de las raíces de g o h, concluya que $\alpha \in \mathbb{F}_p$. [$\frac{1}{2}$ *punto*]

d) Demuestre que en este caso f se descompone en factores lineales en $\mathbb{F}_p[X]$ y deduzca una contradicción. [$\frac{1}{2}$ *punto*]