Universidad de Concepción
Facultad de Ciencias Físicas y Matemáticas
Departamento de Matemática

Listado 08: Campos finitos
Álgebra con Software (527282)

1. ¿Cuántos ideales tiene un campo? ¿Cuáles son?

2. Sean E, F campos y $f : E \to F$ un homomorfismo de anillos. Mostrar que f es inyectivo. *(Indicación: ¿cuál es el kernel de f? Usar el ejercicio anterior.)*

3. Sean E, F campos y $f : E \to F$ un homomorfismo de anillos que sabemos que es inyectivo. Mostrar que el grupo aditivo F^+ puede ser visto como un E-espacio vectorial con el producto escalar dado por $\lambda \cdot x = f(\lambda)x$.

4. Sea E un campo de característica $p > 0$. Sea $\tau : E \to E$ la función definida por $\tau(x) = x^p$. Esta función se conoce como el *morfismo de Frobenius de E*.

   a) Mostrar que τ es un homomorfismo inyectivo de anillos.

   b) Si E es finito, mostrar que τ es un isomorfismo de anillos.

   c) Mostrar que τ es una transformación $\mathbb{F}_p$-lineal.

   d) Si E es finito, mostrar que τ es un isomorfismo de $\mathbb{F}_p$-espacios vectoriales.

5. Sea $E = \mathbb{F}_2[x]/(x^3 + x^2 + 1)$ el campo de 8 elementos. Sea $a \in E$ la clase de x.

   a) Construir la matriz M (con entradas en $\mathbb{F}_2$) que representa la transformación lineal $\tau : E \to E$ dada por $\tau(x) = x^2$ en la base $\{1, a, a^2\}$.

   b) Calcular M^3.

   c) Mostrar cómo los items anteriores implican que todo elemento de E es raíz del polinomio $x^8 - x$.

6. Considerar los campos $E = \mathbb{F}_3[x]/(x^2 + 1)$ y $F = \mathbb{F}_3[x]/(x^2 + x + 2)$, ambos de 9 elementos. Sean $a \in E$ y $b \in F$ las clases de x en cada una de ellas.

   a) Construir un homomorfismo de anillos $\varphi : E \to F$. Mostrar que es un isomorfismo. *(Indicación: hay dos posibles homomorfismos.)*

   b) El código siguiente construye los dos homomorfismos $f, g : E \to F$, construyendo el conjunto X de dichos homomorfismos. Ejecutarlo y descubrir cuál de los dos homomorfismos corresponde al encontrado en el item anterior.

```
x = polygen(GF(3), "x")
E.<a> = GF(3).extension(x^2+1,"a")
F.<b> = GF(3).extension(x^2+x+2, "b")
X = Hom(E,F)
f,g = X
```

   c) Construir el homomorfismo $h = g^{-1} \circ f$ (`h = g.inverse() * f`) con ayuda de Sage. ¿Es un isomorfismo? ¿Entre cuáles estructuras?