

Ejercicios en SAGE: Cálculos en cuerpos finitos y extensiones

Ejercicio 1. Construcción de cuerpos finitos

1. Construí el cuerpo primo $\mathbb{F}_7$.
2. Construí el cuerpo $\mathbb{F}_{3^2}$ como $\mathbb{F}_3[x]/(x^2 + 1)$.
3. Construí el cuerpo $\mathbb{F}_{2^4}$ usando un polinomio irreducible de grado 4 sobre $\mathbb{F}_2$.

Comandos útiles en Sage:

```
GF(p)
GF(p^n, 'a')
```

Ejercicio 2. Elementos primitivos y generadores

1. En $\mathbb{F}_7$, determiná si 3 es generador de $\mathbb{F}_7^*$.
2. Encontrá un elemento primitivo en $\mathbb{F}_{2^4}$.
3. Listá todos los generadores del grupo multiplicativo de $\mathbb{F}_{11}$.

Comandos útiles:

```
F = GF(7)
F.multiplicative_generator()
a.multiplicative_order()
```

Ejercicio 3. Trazas y normas

1. En $\mathbb{F}_{3^3}$, calculá la traza y la norma de un elemento.
2. Repetí el cálculo en $\mathbb{F}_{2^4}$.
3. Verificá que la traza es lineal y que la norma es multiplicativa.

Comandos útiles:

```
x.trace()
x.norm()
```

Ejercicio 4. Bases polinómicas y normales

1. Construí $\mathbb{F}_{3^3}$ como extensión de $\mathbb{F}_3$ con un polinomio irreducible cúbico.
2. Escribí a un elemento cualquiera en la base polinómica estándar $\{1, \alpha, \alpha^2\}$.
3. Determiná si un elemento de $\mathbb{F}_{3^3}$ genera una base normal.

Comandos útiles:

```
S=[a,a^3,a^9]
M=Matrix(GF(3), [[(x*y).trace() for y in S] for x in S])
```

Ejercicio 5. Determinación de base

1. En $\mathbb{F}_{5^2}$, considerá $\{1, \alpha\}$. ¿Es una base de $\mathbb{F}_{25}$ sobre $\mathbb{F}_5$?
2. En $\mathbb{F}_{2^4}$, verificá si $\{1, \alpha^2, \alpha^3, \alpha^5\}$ es una base.

Comando útil:

```
K.vector_space()
```

Ejercicio 6. Estructura de subcampos

1. En $\mathbb{F}_{2^6}$, determiná todos los subcuerpos.
2. Identificá el subcuerpo isomorfo a $\mathbb{F}_{2^3}$.

Comando útil:

```
K.subfields()
```

Ejercicio 7. Polinomios irreducibles

1. Listá todos los polinomios irreducibles de grado 2 en $\mathbb{F}_5[x]$.
2. Verificá la factorización de $x^4 + 1$ en $\mathbb{F}_3[x]$.

Comandos útiles:

```
R.<x> = PolynomialRing(GF(5))
R.irreducible_element(2)
(x^4+1).factor()
```

Ejercicio 8.

- Construí $\mathbb{F}_{2^8}$ (el cuerpo usado en AES en criptografía...próximamente).
- Encontrá un generador de su grupo multiplicativo.
- Calculá la traza y la norma de ese generador sobre $\mathbb{F}_2$.
- Determiná si ese generador da lugar a una base normal.