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

Listado 09: Operaciones en campos finitos
Álgebra con Software (527282)

1. Sean E, F campos con $E \subseteq F$. Sean $p(x) \in E[x]$ un polinomio irreducible con coeficientes en E y $a \in F$ una raíz del polinomio p. Mostrar: si a es raíz de un polinomio $q(x) \in E[x]$, entonces q es múltiplo de p.

2. Usar el ejercicio anterior para mostrar el *teorema de las raíces conjugadas*: si $z \in \mathbb{C} \setminus \mathbb{R}$ es raíz de un polinomio real $p(x) \in \mathbb{R}[x]$, entonces el conjugado $\overline{z}$ también es raíz de p.

3. Determinar, a mano y después con software, los determinantes de cada una de las siguientes matrices. En el caso de que la matriz sea invertible, determinar también su inversa.

   a)
   ```
   R = GF(5)
   M = matrix(R, [[1,3], [3,2]])
   ```

   $$M = \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix}$$

   con coeficientes en el campo R: `Finite Field of size 5`.

   ---

   b)
   ```
   R = GF(7)
   M = matrix(R, [[1,3], [3,2]])
   ```

   $$M = \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix}$$

   con coeficientes en el campo R: `Finite Field of size 7`.

   ---

   c)
   ```
   x = polygen(GF(5), "x")
   R.<a> = GF(5).extension(x^2+x+1, "a")
   M = matrix(R, [[1,a],[a,2*a+1]])
   ```

   $$M = \begin{pmatrix} 1 & a \\ a & 2a+1 \end{pmatrix}$$

   con coeficientes en el campo R: `Finite Field in a of size 5^2` donde a es raíz de $x^2 + x + 1$.

   ---

d)

```
x = polygen(GF(5), "x")
R.<a> = GF(5).extension(x^3+x+1, "a")
M = matrix(R, [[1,a],[a,2*a+1]])
```

$$M = \begin{pmatrix} 1 & a \\ a & 2a+1 \end{pmatrix}$$

con coeficientes en el campo R: `Finite Field in a of size 5^3` donde a es raíz de $x^3 + x + 1$.

4. Determinar, a mano y después con software, los conjuntos solución de cada uno de los siguientes sistemas lineales. Indicar además la cardinalidad de cada conjunto solución.

a)

```
R = GF(7)
M = matrix(R, [[1,2,3],[2,6,2],[5,4,3]])
b = column_matrix(R, [1,5,3])
M_b = M.augment(b, subdivide=True)
```

$$M_b = \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 2 & 6 & 2 & 5 \\ 5 & 4 & 3 & 3 \end{array}\right)$$

con coeficientes en el campo R: `Finite Field of size 7`.

---

b)

```
R = GF(5)
M = matrix(R, [[1,2,3,0],[2,3,2,1],[2,4,3,3]])
b = column_matrix(R, [1,5,3])
M_b = M.augment(b, subdivide=True)
```

$$M_b = \left(\begin{array}{cccc|c} 1 & 2 & 3 & 0 & 1 \\ 2 & 3 & 2 & 1 & 0 \\ 2 & 4 & 3 & 3 & 3 \end{array}\right)$$

con coeficientes en el campo R: `Finite Field of size 5`.

---

c)

```
x = polygen(GF(3), "x")
R.<a> = GF(3).extension(x^2+1, "a")
M = matrix(R, [[1,a,a+2],[2,1,0],[a,a,1]])
b = column_matrix(R, [1,1,1])
M_b = M.augment(b, subdivide=True)
```

$$M_b = \left(\begin{array}{ccr|c} 1 & a & a+2 & 1 \\ 2 & 1 & 0 & 1 \\ a & a & 1 & 1 \end{array}\right)$$

con coeficientes en el campo R: `Finite Field in a of size 3^2` donde a es raíz de $x^2 + 1$.

---

d)

```
x = polygen(GF(3), "x")
R.<a> = GF(3).extension(x^3+2*x+1, "a")
M = matrix(R, [[1,a,a+2],[2,1,0],[a,a,1]])
b = column_matrix(R, [1,1,1])
M_b = M.augment(b, subdivide=True)
```

$$M_b = \left(\begin{array}{ccr|c} 1 & a & a+2 & 1 \\ 2 & 1 & 0 & 1 \\ a & a & 1 & 1 \end{array}\right)$$

con coeficientes en el campo R: `Finite Field in a of size 3^3` donde a es raíz de $x^3 + 2x + 1$.

5. Determinar los polinomios característicos y los valores y vectores propios de cada una de las siguientes matrices. Extender, si es necesario, el campo de coeficientes.

a)

```
R = GF(5)
M = matrix(R, [[1,2,2],[1,1,1],[3,2,1]])
```

$$M = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 1 \\ 3 & 2 & 1 \end{pmatrix}$$

con coeficientes en el campo R: `Finite Field of size 5`.

---

b)

```
R = GF(7)
M = diagonal_matrix(R,[1,6,2,5,2])
M.swap_rows(1,2)
M.swap_rows(3,4)
# Cuidado: swap_rows cuenta las filas desde el cero
```

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 5 & 0 \end{pmatrix}$$

con coeficientes en el campo R: `Finite Field of size 7`.

---

c)

```
x = polygen(GF(7), "x")
R.<a> = GF(7).extension(x^3+2*x+1, "a")
M = matrix(R, [[1,a,0,a+2],[0,a,a,1],
               [1,0,5,3*a],[a,a^2,3,2]])
```

$$M = \begin{pmatrix} 1 & a & 0 & a+2 \\ 0 & a & a & 1 \\ 1 & 0 & 5 & 3a \\ a & a^2 & 3 & 2 \end{pmatrix}$$

con coeficientes en el campo R: `Finite Field in a of size 7^3` donde a es raíz de $x^3 + 2x + 1$.

6. Mostrar: si F es un campo finito, y $f : F \to F$ es un homomorfismo de anillos, entonces f es un isomorfismo de anillos.

7. Para cada campo finito R indicado, se construye el conjunto X de todos los homomorfismos de anillos $R \to R$. Listar y describir los elementos de X. Observando que la composición de dos elementos de X es un elemento de X, construir la tabla de la operación composición entre estos isomorfismos. Finalmente, reconocer cuál de estos isomorfismos corresponde al morfismo de Frobenius.

   a)
   ```
   x = polygen(GF(7), "x")
   R.<a> = GF(7).extension(x^3+2*x+1, "a")
   X = End(R)
   ```

   ---

   b)
   ```
   x = polygen(GF(13), "x")
   R.<a> = GF(13).extension(x^4+x^3+1, "a")
   X = End(R)
   ```

8. En cada caso, determinar si la lista B es una base de Gröbner en el anillo de polinomios P. Si no lo es, construir una base de Gröbner que genere el mismo ideal que el conjunto B.

   a)
   ```
   R = GF(13)
   P.<x,y,t> = PolynomialRing(R, order="lex")
   B = [x^2+y^2-1, y-t*(x+1)]
   ```

   Donde P: $\mathbb{F}_{13}[x, y, t]$ y $B = [x^2 + y^2 + 12, -xt + y - t]$

   ---

   b)
   ```
   x = polygen(GF(7), "x")
   R.<a> = GF(7).extension(x^2+1, "a")
   P.<x,y> = PolynomialRing(R, order="lex")
   B = [x^2+a*y^2+1, x*y+3*a]
   ```

   Donde P: $\mathbb{F}_{7^2}[x, y]$ y $B = [x^2 + ay^2 + 1, xy + 3a]$

9. Sean E, F campos con $E \subseteq F$. Si $|E| = p^k$ y $|F| = p^l$, mostrar: $k \mid l$. *(Indicación: considerar F^+ como un E-espacio vectorial... ¿qué relación hay entre su dimensión y su cardinalidad?)*

10. Utilizando el problema anterior, describir todos los subcampos del campo con 64 elementos

   ```
   R.<a> = GF(2^6, "a")
   ```

Para cada subcampo, determinar un generador.

11. *(Desafío de Software)* Construir un método general para obtener generadores de subcampos de un campo con p^l elementos.

Glosario de comandos útiles

Si M es una matriz:

- `M.echelon_form()` reduce la matriz a su forma reducida escalonada por filas.
- `M.inverse()` invierte la matriz.
- `M.right_kernel()` entrega el kernel de M.
- `M.image()` entrega la imagen de M.
- `M.solve_right(b)`, donde `b` es un vector columna, resuelve el sistema $Mx = b$ (sólo una solución).
- `M.eigenvalues()` entrega una lista con los valores propios de M.
- `M.charpoly()`, `M.minpoly()` entrega, respectivamente, los polinomios característico y minimal de M.

Si E, F son campos:

- `E.frobenius_endomorphism()` entrega el morfismo de Frobenius $E \to E$.
- `Hom(E,F)` construye el conjunto de todos los homomorfismos de campos de E en F.
- `V,f,g = E.vector_space()` construye tres objetos: el espacio vectorial V de las coordenadas de E^+ en la base canónica $\{1, a, a^2, \ldots, a^{d-1}\}$, el isomorfismo de espacios vectoriales $f : V \to E^+$, y su isomorfismo inverso $g : E^+ \to V$.