Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Ejercicios y Problemas resueltos

Tema 1: PRELIMINARES SOBRE ÁLGEBRA LINEAL

Mayo de 2017

Ejercicios Resueltos: Preliminares sobre Álgebra Lineal

1. *Sea $(K, +, \cdot)$ un cuerpo. Demostrar que*

$$K^n = \{(k_1, \ldots, k_n) | k_i \in K, \forall i \in \{1, 2, \ldots, n\}\}$$

con la suma definida por: para cualesquiera $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n$

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

y la multiplicación por un escalar:

$$\forall \lambda \in K, \forall (x_1, \ldots, x_n) \in K^n, \; \lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$$

es un K-espacio vectorial.

Solución

$(K^n, +, .)$ es un K-espacio vectorial ya que

(a) $(K^n, +)$ es un grupo abeliano porque se cumple

i. Asociativa: $\forall (x_1, \ldots, x_n), (y_1, \ldots, y_n), (z_1, \ldots, z_n) \in K^n$, se cumple

$$\begin{array}{l}
((x_1, \ldots, x_n) + (y_1, \ldots, y_n)) + (z_1, \ldots, z_n) = \\
(x_1 + y_1, \ldots, x_n + y_n) + (z_1, \ldots, z_n) = \\
((x_1 + y_1) + z_1, \ldots, (x_n + y_n) + z_n) = \\
(x_1 + (y_1 + z_1), \ldots, x_n + (y_n + z_n)) = \\
(x_1, \ldots, x_n) + (y_1 + z_1, \ldots, y_n + z_n) = \\
(x_1, \ldots, x_n) + ((y_1, \ldots, y_n) + (z_1, \ldots, z_n))
\end{array}$$

por verificarse la propiedad asociativa en $(K, +)$.

ii. Conmutativa: $\forall (x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n$, se cumple

$$\begin{array}{rcl}
(x_1, \ldots, x_n) + (y_1, \ldots, y_n) & = & (x_1 + y_1, \ldots, x_n + y_n) \\
& = & (y_1 + x_1, \ldots, y_n + x_n) \\
& = & (y_1, \ldots, y_n) + (x_1, \ldots, x_n)
\end{array}$$

por verificarse la propiedad conmutativa en $(K, +)$.

iii. Existencia de elemento neutro: Si tomamos el elemento $(0_K, \ldots, 0_K)$ resulta que para todo $(x_1, \ldots, x_n) \in K^n$ se cumple

$$(x_1, \ldots, x_n) + (0_K, \ldots, 0_K) = (x_1 + 0_K, \ldots, x_n + 0_K) = (x_1, \ldots, x_n),$$

por ser 0_K el elemento neutro para $(K, +)$.

iv. Existencia de elemento opuesto: Dado $(x_1, \ldots, x_n) \in K^n$, el elemento $(-x_1, \ldots, -x_n)$ está también en K^n y cumple

$$(x_1, \ldots, x_n)+(-x_1, \ldots, -x_n) = (x_1+(-x_1), \ldots, x_n+(-x_n)) = (0_K, \ldots, 0_K),$$

por lo que existe elemento opuesto.

(b) La multiplicación por un escalar verifica:

i. $1_K(x_1, \ldots, x_n) = (1_K x_1, \ldots, 1_K x_n) = (x_1, \ldots, x_n)$, $\forall (x_1, \ldots, x_n) \in K^n$, por ser 1_K el elemento identidad del cuerpo K.

ii. Para todo $\lambda_1, \lambda_2 \in K$ y $(x_1, \ldots, x_n) \in K^n$, se cumple

$$\begin{aligned}
(\lambda_1 + \lambda_2)(x_1, \ldots, x_n) &= ((\lambda_1 + \lambda_2)x_1, \ldots, (\lambda_1 + \lambda_2)x_n) \\
&= (\lambda_1 x_1 + \lambda_2 x_1, \ldots, \lambda_1 x_n + \lambda_2 x_n) \\
&= (\lambda_1 x_1, \ldots, \lambda_1 x_n) + (\lambda_2 x_1, \ldots, \lambda_2 x_n) \\
&= \lambda_1(x_1, \ldots, x_n) + \lambda_2(x_1, \ldots, x_n)
\end{aligned}$$

por ser $(K, +, .)$ un cuerpo.

iii. Para todo $\lambda \in K$ y $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n$, usando que $(K, +, .)$ es un cuerpo, se tiene

$$\begin{aligned}
\lambda((x_1, \ldots, x_n) + (y_1, \ldots, y_n)) &= \lambda(x_1 + y_1, \ldots, x_n + y_n) \\
&= (\lambda(x_1 + y_1), \ldots, \lambda(x_n + y_n)) \\
&= (\lambda x_1 + \lambda y_1, \ldots, \lambda x_n + \lambda y_n) \\
&= (\lambda x_1, \ldots, \lambda x_n) + (\lambda y_1, \ldots, \lambda y_n) \\
&= \lambda(x_1, \ldots, x_n) + \lambda(y_1, \ldots, y_n).
\end{aligned}$$

iv. Para todo $\lambda_1, \lambda_2 \in K$ y $(x_1, \ldots, x_n) \in K^n$, se tiene

$$\begin{aligned}
(\lambda_1\lambda_2)(x_1, \ldots, x_n) &= ((\lambda_1\lambda_2)x_1, \ldots, (\lambda_1\lambda_2)x_n) \\
&= (\lambda_1(\lambda_2 x_1), \ldots, \lambda_1(\lambda_2 x_n)) \\
&= \lambda_1(\lambda_2 x_1, \ldots, \lambda_2 x_n) \\
&= \lambda_1(\lambda_2(x_1, \ldots, x_n)),
\end{aligned}$$

usando que $(K, +, .)$ es un cuerpo.

2. *Estudiar si los siguientes conjuntos son $\mathbb{F}_q$-subespacios vectoriales de $\mathbb{F}_q^n$ y determinar su dimensión.*

(a) $S_1 = \{(a, a, \ldots, a) \mid a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$.

(b) $S_2 = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid x_n = \sum_{i=1}^{n-1} x_i\}$.

Solución

(a) Observamos que S_1 es no vacío. Usando la Proposición 2.1 del Tema 1, el subconjunto
$$S_1 = \{(a, a, \ldots, a) \mid a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$$
es un $\mathbb{F}_q$-subespacio vectorial si para cualesquiera $\alpha, \beta \in \mathbb{F}_q$ y $(a, a, \ldots, a)$, $(b, b, \ldots, b) \in S_1$, la combinación lineal $\alpha(a, a, \ldots, a) + \beta(b, b, \ldots, b)$ es otro elemento de S_1. Ahora,
$$\alpha(a, a, \ldots, a) + \beta(b, b, \ldots, b) = (\alpha a + \beta b, \alpha a + \beta b, \ldots, \alpha a + \beta b),$$
y como $\alpha, \beta, a, b \in \mathbb{F}_q$ y $\mathbb{F}_q$ es un cuerpo, sabemos que $\alpha a + \beta b$ es otro elemento de $\mathbb{F}_q$, por lo que $(\alpha a+\beta b, \alpha a+\beta b, \ldots, \alpha a+\beta b)$ es un elemento de S_1. Consecuentemente, S_1 es un $\mathbb{F}_q$-subespacio vectorial de $\mathbb{F}_q^n$. Además,
$$(a, a, \ldots, a) = a(1_K, 1_K, \ldots, 1_K),$$
y al se $(1_K, 1_K, \ldots, 1_K)$ un vector no nulo, el conjunto $\{(1_K, 1_K, \ldots, 1_K)\}$ es libre, por lo que una base de S_1 es $\{(1_K, 1_K, \ldots, 1_K)\}$ y es S_1 un subespacio de dimensión 1.

(b) De nuevo, observamos que observamos que S_2 es no vacío. Usando la Proposición 2.1 del Tema 1, el subconjunto
$$S_2 = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid x_n = \sum_{i=1}^{n-1} x_i\}$$
es un $\mathbb{F}_q$-subespacio vectorial si se verifican las dos condiciones siguientes:

i. Para todo $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in S_2$, se tiene
$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) \in S_2.$$

ii. Para todo $\alpha \in \mathbb{F}_q$ y $(x_1, \ldots, x_n) \in S_2$, se cumple $\alpha(x_1, \ldots, x_n) \in S_2$.

En efecto,

i. Como $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in S_2$, sabemos que
$$x_n = \sum_{i=1}^{n-1} x_i \quad y_n = \sum_{i=1}^{n-1} y_i.$$
Por otro lado,
$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$
y
$$x_n + y_n = \sum_{i=1}^{n-1} x_i + \sum_{i=1}^{n-1} y_i = \sum_{i=1}^{n-1} (x_i + y_i)$$
por lo que $(x_1, \ldots, x_n) + (y_1, \ldots, y_n)$ es otro elemento de S_1.

ii. Como $(x_1,\ldots,x_n)\in S_2$, se cumple $x_n=\sum_{i=1}^{n-1}x_i$. Por otro lado, si $\alpha\in\mathbb{F}_q$,

$$\alpha(x_1,\ldots,x_n)=(\alpha x_1,\ldots,\alpha x_n)$$

y

$$\alpha x_n=\alpha\sum_{i=1}^{n-1}x_i=\sum_{i=1}^{n-1}\alpha x_i,$$

luego $\alpha(x_1,\ldots,x_n)\in S_2$.

Además, es fácil ver que el conjunto $\{(1_K,0_K,0_K,\ldots,0_K,1_K), (0_K,1_K,0_K,\ldots,0_K,1_K),\ldots,(0_K,0_K,0_K,\ldots,0_K,1_K,1_K)\}$ es una base de S_2, luego S_2 es de dimensión $n-1$.

3. *Demostrar que el conjunto*

$$\mathcal{B}=\{(1_K,0_K,\ldots,0_K),(0_K,1_K,0_K,\ldots,0_K),\ldots,(0_K,\ldots,0_K,1_K)\}$$

es una base de K^n. ¿Cuál es la dimensión de K^n?

Solución

El conjunto $\mathcal{B}$ será una base de K^n si es un sistema generador de K^n y es libre. Ahora, $\mathcal{B}$ es un sistema generador ya que dado un elemento $(x_1,\ldots,x_n)\in\mathbb{F}_q^n$ se cumple

$$\begin{aligned}(x_1,\ldots,x_n) &= x_1(1_K,0_K,\ldots,0_K)+x_2(0_K,1_K,0_K,\ldots,0_K)+\cdots+\\ &\quad x_n(0_K,\ldots,0_K,1_K).\end{aligned}$$

Además,

$$(0_K,\ldots,0_K)=\alpha_1(1_K,0_K,\ldots,0_K)+\alpha_2(0_K,1_K,0_K,\ldots,0_K)+\cdots+\alpha_n(0_K,\ldots,0_K,1_K)$$

implica

$$0=\alpha_1=\cdots=\alpha_n,$$

por lo que el conjunto $\mathcal{B}$ es también libre. En definitiva, $\mathcal{B}$ es una base de K^n y, por tanto, la dimensión de K^n es precisamente n.

4. *Sea S el subespacio vectorial de $\mathbb{F}_2^7$ definido por*

$$S=<1101000,0110100,0011010,0001101>$$

(a) *Halla una base de S y la dimensión de S.*

(b) *Estudia si la palabra $\mathbf{x}=1000110$ pertenece a S y, en caso de que esté, calcula las coordenadas de $\mathbf{x}$ en la base calculada en el apartado anterior.*

Solución

(a) Por la definición de S, sabemos que

$$T = \{1101000, 0110100, 0011010, 0001101\}$$

es un sistema generador de S. Comprobamos si este conjunto es también libre. Para ello, estudiamos si los únicos escalares de $\mathbb{F}_2$ de una combinación lineal que de el vector 0000000 son todos 0. Tenemos que

$$0000000 = \alpha_1 1101000 + \alpha_2 0110100 + \alpha_3 0011010 + \alpha_4 0001101$$

implica

$$\begin{aligned} 0 &= \alpha_1 \\ 0 &= \alpha_1 + \alpha_2 \\ 0 &= \alpha_2 + \alpha_3 \\ 0 &= \alpha_1 + \alpha_3 + \alpha_4 \ , \\ 0 &= \alpha_2 + \alpha_4 \\ 0 &= \alpha_3 \\ 0 &= \alpha_4 \end{aligned}$$

por lo que la única solución es

$$0 = \alpha_1 = \alpha_2 = \alpha_3 = \alpha_4.$$

Por tanto, T es también libre, luego T es una base S y la dimensión de S es 4.

(b) La palabra $\mathbf{x} = 1000110$ pertenece a S si $\mathbf{x}$ se puede escribir como una combinación lineal de los vectores de la base. Ahora,

$$1000110 = \alpha_1 1101000 + \alpha_2 0110100 + \alpha_3 0011010 + \alpha_4 0001101$$

implica

$$\begin{aligned} 1 &= \alpha_1 \\ 0 &= \alpha_1 + \alpha_2 \\ 0 &= \alpha_2 + \alpha_3 \\ 0 &= \alpha_1 + \alpha_3 + \alpha_4 \ , \\ 1 &= \alpha_2 + \alpha_4 \\ 1 &= \alpha_3 \\ 0 &= \alpha_4 \end{aligned}$$

cuya solución es

$$1 = \alpha_1 = \alpha_2 = \alpha_3 \quad 0 = \alpha_4,$$

esto es,

$$1000110 = 1101000 + 0110100 + 0011010$$

y las coordenadas de 1000110 en la base hallada en el apartado anterior son (1 1 1 0).