7. Seja A uma matriz real $m \times n$ com característica n, e P uma matriz ortogonal tal que $PA = T = \begin{bmatrix} R_{n\times n} \\ 0 \end{bmatrix}$, em que R é uma matriz triangular superior. Mostre que as colunas de X são uma base ortonormada do espaço das colunas de A, onde $P^T = \left[\begin{array}{c|c} X_{m\times n} & Y \end{array}\right]$.

7 $A \in \mathcal{M}_{m\times n}(\mathbb{R})$ tal que $\operatorname{car}(A) = n$

P é ortogonal, logo $P^T = P^{-1}$. Sabemos que as dimensões de P são $m \times m$, para que a multiplicação de $P \cdot A$ esteja definida e pelo facto de P admitir inversa.

$$\boxed{CS(X) \underset{?}{\subseteq} CS(A)}$$

Temos que $PA = T = \begin{bmatrix} R_{n\times n} \\ 0 \end{bmatrix}$ e R é triangular superior e por causa disso invertível.

$$\Rightarrow A = P^T T = P^T \begin{bmatrix} R_{n\times n} \\ 0 \end{bmatrix}$$

Obtemos, desta forma uma fatorização QR de A. onde $Q = P^T$ e $R = T$.

Temos, $P^T = [X_{m\times n} \mid Y]$, pelo que $A = [X \mid Y] \left[\begin{array}{c} R \\ \hline 0 \end{array}\right] = XR$

Seja $v \in CS(X)$. Então existe w: $v = Xw = \underbrace{XR}_{A}R^{-1}w = A(R^{-1}w)$

$\Rightarrow v \in CS(A)$.

$$\boxed{\dim CS(A) \underset{?}{=} \dim CS(X)}$$

Ora, $\dim CS(A) = \operatorname{car}(A) = \operatorname{car}(X) = \dim CS(X)$.

logo $CS(X) = CS(A)$.

8 V espaço vetorial dimensão finita.

V_1 e V_2 subespaços complementares de V.

$$V = V_1 \oplus V_2$$

P projetor sobre V_1 ao longo de V_2

então $Q = I - P$ é projetor sobre V_2 ao longo de V_1.

sabemos que $V_1 = \{v \in V : Pv = v\}$; isto é

$$\left[\begin{array}{l} \text{se } x \in V_1, \text{ então } \operatorname{proj}_{V_1} x = x \text{ e} \\ \text{se } y \in V_2, \text{ então } \operatorname{proj}_{V_1} y = 0 . \end{array}\right]$$

$$\ker(I-P) = \{v \in V : (I-P)v = 0\}$$

$$= \{v \in V : v - Pv = 0\}$$

$$= \{v \in V : Pv = v\} = V_1 .$$

Falta ver que $CS(P) = \ker(I-P)$.

seja $v \in CS(P)$.

Então existe $w \in V$: $Pw = v$

$\Rightarrow (I-P)Pw = (I-P)v$

$\Rightarrow Pw - P^2w = (I-P)v$

$\Rightarrow Pw - Pw = (I-P)v$, por $P^2 = P$ (proj. são idempotentes).

$\Rightarrow (I-P)v = 0$

$\Rightarrow v \in \ker(I-P)$.

Logo $CS(P) \subseteq \ker(I-P)$.

Seja $w \in \ker(I-P)$.

Então $(I-P)w = 0$

$\Rightarrow w - Pw = 0$

$\Rightarrow w = Pw$

$\Rightarrow w \in CS(P)$.

Logo $\ker(I-P) \subseteq CS(P)$, pelo que $CS(P) = \ker(I-P)$.

Seja $Q = I-P$ projetor.

$$CS(I-P) \underset{\substack{\uparrow \\ \text{por def de } Q}}{=} CS(Q) \underset{\substack{\uparrow \\ \text{pela dem. anterior}}}{=} \ker(I-Q) \underset{\substack{\uparrow \\ \text{por def de } Q}}{=} \ker(P) \underset{\substack{\uparrow \\ \text{por def.}}}{=} V_2$$

$\ker(I-Q) = \{v \in V : (I-Q)v = 0\} = \{v \in V : Qv = v\} = V_2$.

1. Considere o primo $p = 200131$. Defina uma curva elíptica E sobre os inteiros módulo p. Usando parâmetros à sua escolha, use o sistema Menezes-Vanstone para cifrar `mens=(51101, 10112)` na curva elíptica E. Conhecendo a chave privada, decifre o que cifrou.

3. Alice e Bob acordaram na curva elíptica E definida por $y^2 = x^3 + 338271x + 1435547$ sobre $\mathbb{Z}_{5894177}$. Irão usar o protocolo de Massey-Omura. Explique como pode Alice enviar a mensagem `mens=123` a Bob. Determine o texto cifrado e descreva todos os passos que seguiu, supondo que a forma de transformar a mensagem no ponto da curva elíptica é a proposta por Koblitz. Explique, detalhadamente, como Bob obtem a mensagem original `mens=123` do criptograma recebido.

Confirmar se perguntas 2 e 5 não saem mesmo.

4. Mostre, detalhadamente, que $\left(\frac{13}{233}\right) = 1$. Calcule, usando o algoritmo estudado nas aulas, uma raiz quadrada de 13 módulo 233.

$$\left(\frac{13}{233}\right) = (-1)^{\overbrace{\frac{13-1}{2}}^{} \cdot \frac{233-1}{2}} \left(\frac{233}{13}\right)$$

par

$$233 = 13 \cdot 17 + 12$$

13, 26, 39, 52, 65, 78, 91, 104

$$= \left(\frac{12}{13}\right) = \left(\frac{2^2}{13}\right)\left(\frac{3}{13}\right)$$

$$= \left(\frac{2}{13}\right)^2 \left(\frac{3}{13}\right)$$

$$\boxed{\left(\frac{2}{13}\right) = -1, \text{ pq } 13 \equiv -3 \pmod 8}$$

$$= (-1)^{\frac{3-1}{2} \cdot \underbrace{\frac{13-1}{2}}_{\text{par}}} \left(\frac{13}{3}\right)$$

$$= \left(\frac{1}{3}\right) = 1^{\frac{3-1}{2}} = 1$$

$$\left[\mathbb{Z}_{233}[x] \Big/ x^2 - 13 = \{\alpha x + \beta : \alpha, \beta \in \mathbb{Z}_{233}\}\right]$$

Pelo algoritmo das aulas

180 e 53 são resíduos quadráticos de 13.