- 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 $P^T=$ $| X_{m \times n} | Y |$.
- A E Mmin (R) tal que con (A)=n

Pé ontogonal, logo PT = PT. Sabernos que as dimensõs de P são mxm, poro que a multiplicação de P.A estija definido o pelo facto de P admitin invensa.

 $CS(X) \subseteq CS(A)$

The que $PA = T = \begin{bmatrix} R_{n \times n} \end{bmatrix}$ e R i margher superion a por cause disso invertial.

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

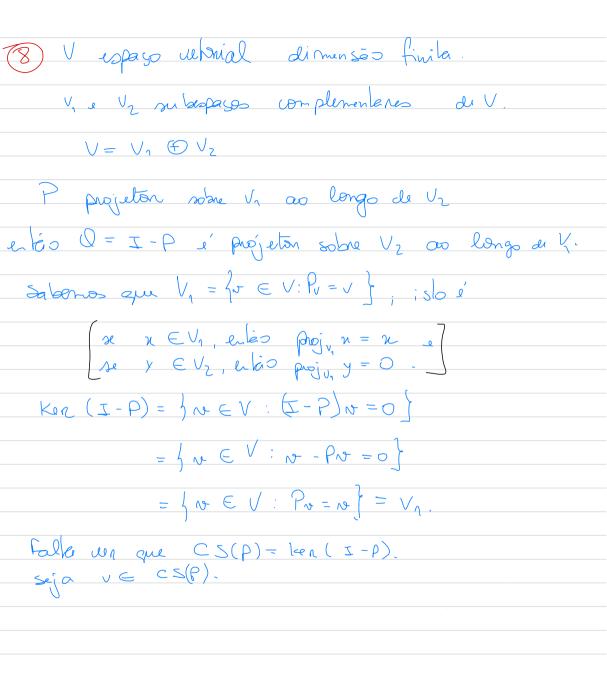
Obtemos desta forme umo fatoritação QR de A orde Q = PT e R = T.

Tenos, PT = [Xmxn | Y], pelo que A = [X | Y] [R] = XR Seja $oldsymbol{oldsymbol$

dim CS(A)= dim CS(X)

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

logo CS(X) = CS(A).



Grido existe
$$w \in V$$
: $Pw = V$

$$\Rightarrow (z-P)Pw = (z-P)V$$

$$\Rightarrow Pw-Pw = (z-P)V$$

$$\Rightarrow (z-P)V = 0$$

$$\Rightarrow V \in Ken(z-P).$$
Sign $e \in Ken(z-P)$

$$\Rightarrow w = Pw$$

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

logo Kan (I-P) < CS(P) plo que (S(P)=bn(I-P).

Sign
$$Q = I - P$$
 projeton.
 $CS(I - P) = (S(Q) = \text{ker}(I - Q) = \text{ker}(P) = V_2$

pan def de pelo dem antaion por def de Q .

 Q
 $\text{ker}(I - Q) = \{v \in V : (I - Q)v = 0\} = \{v \in V : Q_V = v\} = V_Z$

- 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.

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

$$\frac{A_{3}}{2_{33}} = (-1)^{\frac{13-1}{2}} \frac{2_{33}}{4_{3}} \qquad \frac{A_{3}}{4_{3}} \qquad \frac{A_{3}$$

$$\left[\mathbb{Z}_{233}\left[n\right]_{n^2-13}=\left\{\alpha n+\beta:\alpha,\beta\in\mathbb{Z}_{273}\right\}\right]$$

Pelo algoritmo das aules

180 e 53 são residues quedrátios de 13,