V9 LINEAR ALGEBRA REVIEW

- VECTOR SPACES (OVER FINITE FIELDS)
- MATRICES

VECTOR SPACES

- Let $F = GF(q)$.
- $V_n(F) = \underbrace{F \times F \times \cdots \times F}_{n} = F^n = \{(x_1, x_2, \ldots, x_n) : x_i \in F\}$ is an n-dimensional vector space over F, where

  addition is $(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1+y_1, x_2+y_2, \ldots, x_n+y_n)$

  and scalar multiplication is $\lambda \cdot (x_1, x_2, \ldots, x_n) = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$.

- A subset $C \subseteq V_n(F)$ is a vector subspace of $V_n(F)$ if:
  - (i) C is non-empty;
  - (ii) C is closed under addition: $\forall x, y \in C$, $x+y \in C$;
  - (iii) C is closed under scalar multiplication: $\forall x \in C, \forall \lambda \in F$, $\lambda \cdot x \in C$.

- Note: A vector subspace of $V_n(F)$ is also a vector space over F.

LINEAR INDEPENDENCE

- Let C be a vector space over $F = GF(q)$, and let $v_1, v_2, \ldots, v_k \in C$.
- A linear combination of $v_1, v_2, \ldots, v_k$ is a vector in C:

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k, \quad \text{where } \lambda_i \in F.$$

- The span of $\{v_1, v_2, \ldots, v_k\}$ is $\mathrm{Span}(v_1, \ldots, v_k) = \{\lambda_1 v_1 + \cdots + \lambda_k v_k : \lambda_i \in F\}$.

  Note: $\mathrm{Span}(v_1, \ldots, v_k) \subseteq C$.

- The vectors $v_1, v_2, \ldots, v_k$ are linearly independent over F if the only solution to $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k = 0$ is $\lambda_1 = \lambda_2 = \cdots = \lambda_k = 0$; otherwise, the vectors are linearly dependent over F.

- If $v_1, v_2, \ldots, v_k$ are l.i. over F, then $|\mathrm{Span}(v_1, \ldots, v_k)| = q^k$; otherwise, $|\mathrm{Span}(v_1, \ldots, v_k)| < q^k$.

BASES AND DIMENSION

- Let C be a vector space over $F = GF(q)$.
- A basis of C is a linearly independent set $\{v_1, v_2, \ldots, v_k\} \subseteq C$, with $\mathrm{Span}(v_1, v_2, \ldots, v_k) = C$.

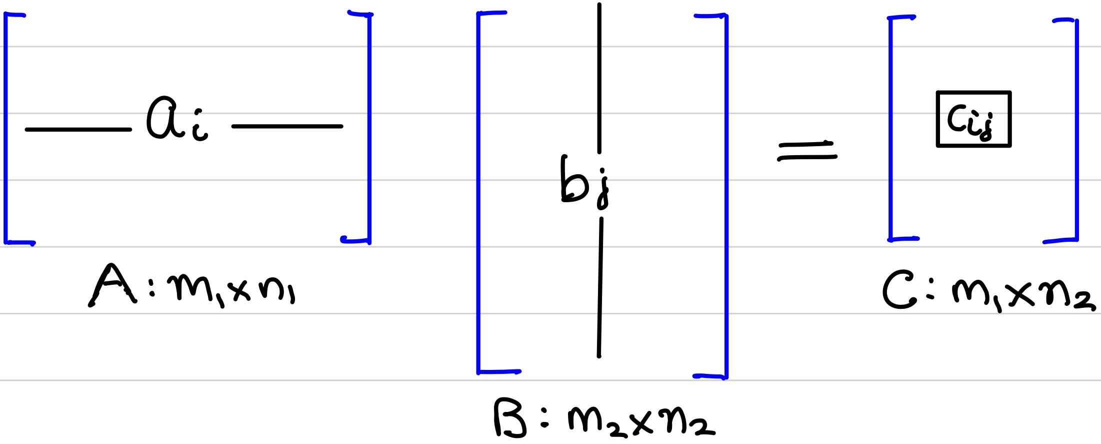
- FACTS 1) C has a basis.
  2) All bases of C have the same size, called the dimension of C.
  3) If $\dim(C) = k$, then $|C| = q^k$.

- Note: $C = \{0\}$ is a 0-dimensional vector space over F, with basis $\{\ \}$.

MATRICES

- **Addition and Subtraction**: Let $A=[a_{ij}]$ and $B=[b_{ij}]$ be $m\times n$ matrices over F. Then $A+B=[a_{ij}+b_{ij}]$ and $A-B=[a_{ij}-b_{ij}]$.

- **Multiplication**: Let $A_{m_1\times n_1}$ and $B_{m_2\times n_2}$ be matrices over F. Then $A\cdot B$ is only defined if $n_1=m_2$, in which case $A\cdot B$ has dimensions $m_1\times n_2$:



EXAMPLE Let $C \subseteq V_n(F)$ be a vector space over F with basis $\{v_1, v_2, \ldots, v_k\}$. Then C can be defined by the $k \times n$ matrix

$$G = \begin{bmatrix} \text{———} & v_1 & \text{———} \\ \text{———} & v_2 & \text{———} \\ & \vdots & \\ \text{———} & v_k & \text{———} \end{bmatrix}.$$

Note that $C = \{[m_1, m_2, \ldots, m_k] \cdot G : [m_1, m_2, \ldots, m_k] \in V_k(F)\}$
$= \{m_1 v_1 + m_2 v_2 + \cdots + m_k v_k : [m_1, m_2, \ldots, m_k] \in V_k(F)\}$
$=$ row space of G.

RANK OF A MATRIX

- Let A be an $m \times n$ matrix over F.
- The row space of A is the vector subspace of $V_n(F)$ spanned by the rows of A. The row rank of A is the dimension of its row space.
- The column space of A is the vector subspace of $V_m(F)$ spanned by the columns of A. The column rank of A is the dimension of its column space.
- FACT : The row rank and column rank of A are equal, and is called the rank of A.

EXAMPLE Determine the dimension of the vector subspace C of $V_5(\mathbb{Z}_5)$ that is spanned by $v_1=(3,0,2,3,1)$, $v_2=(2,1,3,4,0)$, $v_3=(0,4,3,1,1)$, and $v_4=(2,1,1,2,2)$.

SOLUTION

Let $G = \begin{bmatrix} 3 & 0 & 2 & 3 & 1 \\ 2 & 1 & 3 & 4 & 0 \\ 0 & 4 & 3 & 1 & 1 \\ 2 & 1 & 1 & 2 & 2 \end{bmatrix}_{4\times 5}$. Then $\dim(C) = \operatorname{rank}(G)$.

Use elementary row operations to determine the (reduced) row echelon form of G:

$$\xrightarrow{R_1 \leftarrow 2R_1} \begin{bmatrix} 1 & 0 & 4 & 1 & 2 \\ 2 & 1 & 3 & 4 & 0 \\ 0 & 4 & 3 & 1 & 1 \\ 2 & 1 & 1 & 2 & 2 \end{bmatrix} \xrightarrow[R_4 \leftarrow R_4 - 2R_1]{R_2 \leftarrow R_2 - 2R_1}$$

$$\begin{bmatrix} 1 & 0 & 4 & 1 & 2 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 4 & 3 & 1 & 1 \\ 0 & 1 & 3 & 0 & 3 \end{bmatrix} \xrightarrow[R_4 \leftarrow R_4 - R_2]{R_3 \leftarrow R_3 - 4R_2} \begin{bmatrix} 1 & 0 & 4 & 1 & 2 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 3 & 3 & 2 \\ 0 & 0 & 3 & 3 & 2 \end{bmatrix}$$

$$\xrightarrow{R_4 \leftarrow R_4 - R_3} \begin{bmatrix} 1 & 0 & 4 & 1 & 2 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 3 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Hence $\operatorname{rank}(G) = 3$, so $\underline{\dim(C) = 3.}$

NULL SPACE AND INVERTIBILITY

- Let A be an $m \times n$ matrix over F.
- The null space of A is $\{x \in V_n(F) : Ax^T = 0\}$.
- The null space of A is a vector subspace of $V_n(F)$; its dimension is called the nullity of A.
- FACT $\operatorname{rank}(A) + \operatorname{nullity}(A) = n$.

- Let A be an $n \times n$ matrix over F. A is invertible (or non-singular) if there exists an $n \times n$ matrix B over F with $AB = BA = I_n$; we write $B = A^{-1}$.
- FACT A is invertible $\Longleftrightarrow$ A has rank n $\Longleftrightarrow$ $\det(A) \neq 0$.