4th Class:

I: Vector spaces: Abstraction of space $\mathbb{R}^n$; i.e. A space where vector addition & scalar product can be defined.

Formally, a vector space V over a field $\mathbb{F}$ is given by a triplet $(T, +, \cdot)$ s.t. $(T, +)$ commutative group & $\cdot$, referred as scalar product, is a function from $F \times T \to T$ s.t. $\forall\, a, b \in F$ & $u, v \in T$, $(a+b)\cdot u = a\cdot u + b\cdot u$

$$a\cdot(u+v) = a\cdot u + a\cdot v.$$

Eg: for any field, F, F^n forms a vector space where $+$ is coordinate wise sum & scalar product is coordinate-wise scaling.

Linear Supspace: A non-empty $S \subseteq F^n$ is called linear supspace if is closed under vector-addition & scalar product.

Many definitions & properties also extends from $\mathbb{R}^n$ to F^n for any field.

Span: For any set $B = \{v_1, \ldots, v_\ell\}$,
$$\text{span}(B) = \left\{ \sum_{i=1}^{\ell} a_i \cdot v_i \mid a_i \in F \right\}$$

Linear (in)dependence: $v_1, \ldots, v_\ell$ are linearly independent, if $\forall\ i \in [\ell]$ & $(a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k) \in F^{k-1}$,
$$v_i \neq a_1 v_1 + \cdots + a_{i-1} v_{i-1} + a_{i+1} v_{i+1} + \cdots + a_\ell v_\ell .$$
i.e., $v_i \notin \text{span}(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_\ell)$.

Otherwise, $v_1, \ldots, v_\ell$ are linearly dependent.

Basis & Dimension: For a vector space V over F, $B \subseteq V$ is called a basis for V, if vectors in B are linearly independent & $V = \text{span}(B)$. Cardinality of any two basis set is same, it is called dimension of B.

Rank of matrix: $M \in F^{k \times n}$

row-rank(M) = maximum number of linearly independent rows.

column-rank(M) = maximum number of linearly independent columns.

$$\text{row-rank}(M) = \text{column-rank}(M) = \text{rank}(M).$$

M is full-rank if $\text{rank}(M) = \min\{k, n\}$.

Rank-nullity Theorem: $M \in F^{k \times n}$.

$M : F^n \longrightarrow F^k$ s.t $a \in F^n \longmapsto Ma$.

$\text{null-space}(M) = \{v \in F^n : Mv = 0\}$.

$\text{rank}(M) + \dim(\text{null-space}(M)) = n$.

Theorem: Let $S \subseteq \mathbb{F}_q^n$ is a linear supspace. Then

1. $|S| = q^k$ where $k = \dim(S)$.
2. $\exists$ a full-rank matrix $G \in \mathbb{F}_q^{k \times n}$ s.t.
   $S = \{\bar{a}^T \cdot G \mid a \in \mathbb{F}_q^k\}$. (Generator matrix)
3. $\exists$ full rank matrix $H \in \mathbb{F}_q^n$ s.t.
   $S = \{a \in \mathbb{F}_q^n \mid H \cdot a = 0\}$.
4. G & H are othogonal s.t. $G \cdot H^T = 0$.

(Exercise).

Lemma: Let $G \in \mathbb{F}_q^{k \times n}$ be a generator matrix for the supspace S_1 & $H \in \mathbb{F}_q^{n-k \times n}$ is parity check matrix for a space S_2 s.t $G \cdot H^T = 0$. Then $S_1 = S_2$.

(Exercise)