EE 441: General vector spaces over a field

I. Axioms for a Vector Space $\mathcal{V}$ over a Field $\mathbb{F}$

Let $\mathbb{F}$ be a general field. Let $\mathcal{V}$ be a set of objects called "vectors." We say that $\mathcal{V}$ is a *vector space over the field* $\mathbb{F}$ if there are rules for vector addition and scalar multiplication such that $\mathcal{V}$ is closed with respect to these operations, that is:

- $\boldsymbol{v}_1 + \boldsymbol{v}_2 \in \mathcal{V}$ for any two vectors $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathcal{V}$.
- $\alpha\boldsymbol{v} \in \mathcal{V}$ for any vector $\boldsymbol{v} \in \mathcal{V}$ and any scalar $\alpha \in \mathbb{F}$.

and such that the following additional six properties hold:

1) (Commutativity)
$$\boldsymbol{v}_1 + \boldsymbol{v}_2 = \boldsymbol{v}_2 + \boldsymbol{v}_1 \quad \text{(for all } \boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathcal{V}\text{)}$$
2) (Associativity)
$$(\boldsymbol{v}_1 + \boldsymbol{v}_2) + \boldsymbol{v}_3 = \boldsymbol{v}_1 + (\boldsymbol{v}_2 + \boldsymbol{v}_3) \quad \text{(for all } \boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3 \in \mathcal{V}\text{)}$$
$$(\alpha\beta)\boldsymbol{v} = \alpha(\beta\boldsymbol{v}) \quad \text{(for all } \alpha, \beta, \in \mathbb{F} \text{ and } \boldsymbol{v} \in \mathcal{V}\text{)}$$
3) (Distributive Properties)
$$\alpha(\boldsymbol{v}_1 + \boldsymbol{v}_2) = \alpha\boldsymbol{v}_1 + \alpha\boldsymbol{v}_2 \quad \text{(for all } \boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathcal{V}\text{, and } \alpha \in \mathbb{F}\text{)}$$
$$(\alpha + \beta)\boldsymbol{v} = \alpha\boldsymbol{v} + \beta\boldsymbol{v} \quad \text{(for all } \boldsymbol{v} \in \mathcal{V}\text{, and } \alpha, \beta \in \mathbb{F}\text{)}$$
4) (Additive Identity) There exists a vector $\boldsymbol{0} \in \mathcal{V}$ such that:
$$\boldsymbol{v} + \boldsymbol{0} = \boldsymbol{v} \quad \text{for all } v \in \mathcal{V}$$
5) (Additive Inverse) For every $\boldsymbol{v} \in \mathcal{V}$, there exists a vector $-\boldsymbol{v} \in \mathcal{V}$ such that:
$$\boldsymbol{v} + -\boldsymbol{v} = \boldsymbol{0}$$
6) (Multiplicative Identity) $1\boldsymbol{v} = \boldsymbol{v}$ for every vector $\boldsymbol{v} \in \mathcal{V}$.

Note that the vector space $\mathbb{R}^n$ over the field $\mathbb{R}$ satisfies all these properties. Similarly, the set $\mathbb{F}^n$ is a vector space over $\mathbb{F}$, where vector addition and scalar multiplication are defined entrywise via the arithmetic of $\mathbb{F}$. Other examples of vector spaces:

- The vector space $\mathcal{V}$ over the field $\mathbb{F}$ (where $\mathbb{F}$ is any general field), consisting of all countably infinite tuples $(x_1, x_2, x_3, \ldots)$, where $x_i \in \mathbb{F}$ for all entries $i \in \{1, 2, \ldots, \}$, and where arithmetic is defined entrywise using arithmetic in $\mathbb{F}$.
- The vector space $\mathcal{V}$ over the field $\mathbb{R}$, where $\mathcal{V}$ is the set of all continuous functions of time t for $t \in (-\infty, \infty)$.
- The vector space $\mathcal{V}$ over the field $\mathbb{R}$, where $\mathcal{V}$ is the set of all polynomial functions $f(t)$ of degree less than or equal to n. That is, $\mathcal{V} = \{f(t) \mid f(t) = \alpha_0 + \alpha_1 t + \alpha_2 t^2 + \ldots + \alpha_n t^n, \alpha_i \in \mathbb{R}\}$.

II. Simple Lemmas for Vector Spaces

Let $\mathcal{V}$ be a vector space over a field $\mathbb{F}$.

Lemma 1: (Uniqueness of $\boldsymbol{0}$) The vector $\boldsymbol{0} \in \mathcal{V}$ is the unique additive identity.

Proof: Suppose that $\boldsymbol{w}$ satisfies $\boldsymbol{v} + \boldsymbol{w} = \boldsymbol{v}$ for any $\boldsymbol{v} \in \mathcal{V}$. Then adding $-\boldsymbol{v}$ to both sides of the equation $\boldsymbol{v} + \boldsymbol{w} = \boldsymbol{v}$ yields:
$$-\boldsymbol{v} + \boldsymbol{v} + \boldsymbol{w} = -\boldsymbol{v} + \boldsymbol{v}$$
and hence: $\boldsymbol{0} + \boldsymbol{w} = \boldsymbol{0}$. Therefore, $\boldsymbol{w} = \boldsymbol{0}$. □

Lemma 2: (Uniqueness of $-\boldsymbol{v}$) For any vector $\boldsymbol{v} \in \mathcal{V}$, if there is a vector $\boldsymbol{w} \in \mathcal{V}$ such that $\boldsymbol{v} + \boldsymbol{w} = \boldsymbol{0}$, then $\boldsymbol{w} = -\boldsymbol{v}$.

Proof: Suppose that $\boldsymbol{v} + \boldsymbol{w} = \boldsymbol{0}$. Adding $-\boldsymbol{v}$ to both sides yields $\boldsymbol{0} + \boldsymbol{w} = -\boldsymbol{v}$, and hence $\boldsymbol{w} = -\boldsymbol{v}$. □

Lemma 3: $0\boldsymbol{v} = \boldsymbol{0}$ for any $\boldsymbol{v} \in \mathcal{V}$.

Proof: Take any vector $\boldsymbol{v} \in \mathcal{V}$. Then:
$$\boldsymbol{v} = 1\boldsymbol{v} = (1 + 0)\boldsymbol{v} = 1\boldsymbol{v} + 0\boldsymbol{v}$$
and hence $\boldsymbol{v} = \boldsymbol{v} + 0\boldsymbol{v}$. Adding $-\boldsymbol{v}$ to both sides yields $\boldsymbol{0} = 0\boldsymbol{v}$, proving the result. □

Lemma 4: $\alpha\mathbf{0} = \mathbf{0}$ for any $\alpha \in \mathbb{F}$.

Proof: Take any $\alpha \in \mathbb{F}$ and any vector $\boldsymbol{v} \in \mathcal{V}$. Then:

$$\begin{aligned} \alpha\boldsymbol{v} &= \alpha(\boldsymbol{v} + \mathbf{0}) \\ &= \alpha\boldsymbol{v} + \alpha\mathbf{0} \end{aligned}$$

Thus, we have $\alpha\boldsymbol{v} = \alpha\boldsymbol{v} + \alpha\mathbf{0}$. Adding $-(\alpha\boldsymbol{v})$ to both sides yields $\mathbf{0} = \alpha\mathbf{0}$, proving the result. □

Lemma 5: $-\boldsymbol{v} = (-1)\boldsymbol{v}$ for any $\boldsymbol{v} \in \mathcal{V}$.

Proof: Take any vector $\boldsymbol{v} \in \mathcal{V}$. Then:

$$\mathbf{0} = 0\boldsymbol{v} = (1 + -1)\boldsymbol{v} = 1\boldsymbol{v} + (-1)\boldsymbol{v} = \boldsymbol{v} + (-1)\boldsymbol{v}$$

Thus, $\mathbf{0} = \boldsymbol{v} + (-1)\boldsymbol{v}$. Adding $-\boldsymbol{v}$ to both sides yields $-\boldsymbol{v} = (-1)\boldsymbol{v}$, proving the result. □

III. SUBSPACES

Definition 1: Let $\mathcal{V}$ be a vector space over a field $\mathbb{F}$. Let $\mathcal{S} \subset \mathcal{V}$ be a subset of $\mathcal{V}$. We say that $\mathcal{S}$ is a *subspace* if:

$$\begin{aligned} \boldsymbol{v}_1 + \boldsymbol{v}_2 \in \mathcal{S} \quad & \text{for all } \boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathcal{S} \\ \alpha\boldsymbol{v} \in \mathcal{S} \quad & \text{for all } \boldsymbol{v} \in \mathcal{V},\ \alpha \in \mathbb{F} \end{aligned}$$

where addition and scalar multiplication are the same in $\mathcal{S}$ as they are in $\mathcal{V}$.

It is easy to prove that if $\mathcal{S}$ is a subspace of vector space $\mathcal{V}$ over field $\mathbb{F}$, then $\mathcal{S}$ is *itself* a vector space over field $\mathbb{F}$. (It is important to note that $-\boldsymbol{v} = (-1)\boldsymbol{v}$ in proving this...why?).

IV. LINEAR COMBINATIONS AND LINEAR INDEPENDENCE

Definition 2: Let $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ be a collection of vectors in a vector space $\mathcal{V}$ over a field $\mathbb{F}$. We say that a vector $\boldsymbol{v} \in \mathcal{V}$ is a *linear combination* of $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ if it can be written: $\boldsymbol{v} = \alpha_1\boldsymbol{x}_1 + \ldots + \alpha_k\boldsymbol{x}_k$ for some scalars $\alpha_i \in \mathbb{F}$ for $i \in \{1, \ldots, k\}$.

Definition 3: Let $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ be a collection of vectors in a vector space $\mathcal{V}$ over a field $\mathbb{F}$. We define $Span\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ as the set of all linear combinations of $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$. Note that $Span\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\} \subset \mathcal{V}$.

Definition 4: Let $\mathcal{S}$ be a subspace of a vector space $\mathcal{V}$ over a field $\mathbb{F}$. We say that a collection of vectors $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ *span* $\mathcal{S}$ if $Span\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\} = \mathcal{S}$.

Definition 5: We say that a collection of vectors $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ in a vector space $\mathcal{V}$ (over a field $\mathbb{F}$) are *linearly independent* if the equation $\alpha_1\boldsymbol{v}_1 + \alpha_2\boldsymbol{v}_2 + \ldots + \alpha_k\boldsymbol{v}_k = \mathbf{0}$ can only be true if $\alpha_i = 0$ for all $i \in \{1, \ldots, k\}$.

Definition 6: A collection of vectors $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ is a *basis for a subspace* $\mathcal{S}$ if the collection $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ is linearly independent in $\mathcal{S}$ and spans $\mathcal{S}$.

The following lemmas have proofs that are identical (or nearly identical) to the corresponding lemmas proven in class for the vector space $\mathbb{R}^n$. The proofs are left as an exercise.

Lemma 6: A collection of vectors $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ are linearly independent if and only if none of the vectors can be written as a linear combination of the others.

Lemma 7: If $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ are linearly independent in a vector space $\mathcal{V}$, and if $\boldsymbol{w} \in \mathcal{V}$ and $\boldsymbol{w} \notin Span\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$, then $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k, \boldsymbol{w}\}$ are linearly independent.

Lemma 8: ($k \leq m$) Let $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ be a collection of vectors that are linearly independent in a subspace $\mathcal{S}$. Let $\{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m\}$ be a collection of vectors that span $\mathcal{S}$. Then $k \leq m$.

Lemma 9: Any two bases of a subspace $\mathcal{S}$ have the same size, defined as the *dimension* of the subspace.

Lemma 10: The dimension of $\mathbb{F}^n$ is n.

Lemma 11: Let $\mathcal{S}$ be a subspace of a vector space $\mathcal{V}$, where $\mathcal{V}$ has dimension n. Then $\mathcal{S}$ has a finite basis, and the dimension of $\mathcal{S}$ is less than or equal to n.

Note that the *standard basis* for $\mathbb{F}^n$ is given by $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$, where $\boldsymbol{e}_i$ is a n-tuple with all entries equal to 0 except for entry i, which is equal to 1.

Note that the collection $\{1, t, t^2, \ldots, t^n\}$ is a basis for the vector space $\mathcal{V}$ over the field $\mathbb{R}$, where $\mathcal{V}$ is the space of all polynomial functions of degree less than or equal to n (why is this true?). Thus, this vector space has dimension $n+1$. Note also that, for any n, this vector space is a *subspace* of the vector space over $\mathbb{R}$ defined by all continuous functions. Thus, the dimension of the vector space of all continuous functions is infinite (as it contains subspaces of dimension n for arbitrarily large n).

V. Matrices

Let A be a $m \times n$ matrix with elements in $\mathbb{F}$. Note that the equation $A\boldsymbol{x} = \boldsymbol{0}$ (where $\boldsymbol{0} \in \mathbb{F}^m$ and $\boldsymbol{x} \in \mathbb{F}^n$) has only the trivial solution $\boldsymbol{x} = \boldsymbol{0} \in \mathbb{F}^n$ if and only if the columns of A are linearly independent.

Lemma 12: A square $n \times n$ matrix A (with elements in $\mathbb{F}$) is non-singular if and only if its columns are linearly independent, if and only if $A\boldsymbol{x} = \boldsymbol{0}$ has only the trivial solution.

The above lemma follows from the fact that if A is non-singular, it has a single unique solution to $A\boldsymbol{x} = \boldsymbol{b}$ for all $\boldsymbol{b} \in \mathbb{F}^n$ (which is true by Gaussian Elimination), and if it is singular it does not have a solution for some vectors $\boldsymbol{b} \in \mathbb{F}^n$ and it has multiple solutions for the remaining $\boldsymbol{b} \in \mathbb{F}^n$.

Lemma 13: Let A, B be square $n \times n$ matrices. If $AB = I$, then both A and B are invertible, and $A^{-1} = B$ and $B^{-1} = A$. The above lemma follows from the fact that $AB = I$ implies A is non-singular (why?) and hence invertible.

Lemma 14: A square $n \times n$ matrix A (with elements in $\mathbb{F}$) has linearly independent columns (and hence is invertible) if and only if its transpose A^T has linearly independent columns (and hence is invertible). Thus, a square invertible matrix A has both linearly independent rows and linearly independent columns.

The above lemma follows from the fact that $AA^{-1} = I$, and hence $(A^{-1})^T A^T = I$.

VI. Basic Probability

The next several lectures on erasure coding will use the following simple but important probability facts:

- If a probability experiment has K equally likely outcomes, then the probability of each individual outcome is $1/K$.
- Let $E_1, E_2, \ldots, E_m$ be a set of independent events (say, from m independent probability experiments). Then:

  $$Pr[E_1 \cap E_2 \cap \cdots \cap E_m] = Pr[E_1]Pr[E_2] \cdots Pr[E_m]$$

  That is, the probability that all independent events occur is equal to the product of the individual event probabilities.
- (Union Bound) Let $E_1, E_2, \ldots, E_m$ be a collection of m events (possibly not independent). Then:

  $$Pr[E_1 \cup E_2 \cup \cdots \cup E_m] \leq \sum_{i=1}^{m} Pr[E_i]$$

  That is, the probability that at least one of the events occurs is less than or equal to the sum of the individual event probabilities.