1. **Linear algebra fundamentals.**

A **group** is a set \( G \) and associative binary operation \( \ast \) with
- **closure**: \( a, b \in G \Rightarrow a \ast b \in G \)
- **identity**: \( \exists e \in G \) such that \( a \ast e = e \ast a = a \ \forall a \in G \)
- **inverse**: \( \forall a \in G, \exists b \) such that \( a \ast b = b \ast a = e \).

A group is **abelian** (or **commutative**) if \( a \ast b = b \ast a \ \forall a, b \in G \).

**Def:** A **field** is a set \( F \) containing \( 1 \neq 0 \) with two binary operations, \( + \) (addition) and \( \ast \) (multiplication) such that
(i) \( F \) is an abelian group under addition
(ii) \( F \setminus \{0\} \) is an abelian group under multiplication
(iii) The distributive law holds: \( a(b + c) = ab + ac \ \forall a, b, c \in F \).

**Examples:** \( \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p \) (prime \( p \)) are all fields.

\( \mathbb{Z} \) is not a field.

**Note:** The additive identity is \( 0 \), and the inverse of \( a \) is \(-a\).

The multiplicative identity is \( 1 \), and the inverse of \( a \) is \( a^{-1} \) or \( \frac{1}{a} \).

**Def:** A **linear space** (or **vector space**), is a set \( X \) (of vectors) over a field \( F \) (of scalars) such that
(i) \( X \) is an abelian group under addition
(ii) Addition & multiplication are "compatible" in that they have
natural associative & distributive laws relating the two:

- \( a(v+w) = av + aw \quad \forall a \in F, \quad v, w \in X. \)
- \( (a+b)v = av + bv \quad \forall a, b \in F, \quad v, w \in X. \)
- \( a(bv) = (ab)v \quad \forall a, b \in F, \quad v \in X. \)
- \( 1v = v \quad \forall v \in X. \)

Think of a vector space as a set of vectors that is

(i) closed under addition & inverses
(ii) closed under scalar multiplication
(iii) equipped with the "natural" associative & distributive laws.

Prop: In any vector space \( X \),

(i) The zero vector \( 0 \) is unique
(ii) \( 0x = 0 \) for all \( x \in X \)
(iii) \( -1x = -x \) for all \( x \in X \).

Pf: Exercise (easy). \( \square \)

Def: A linear map between vector spaces \( X \) and \( Y \) over \( K \) is a function \( \phi: X \to Y \) satisfying

(i) \( \phi(v+w) = \phi(v) + \phi(w) \quad \forall v, w \in X \)
(ii) \( \phi(av) = a \phi(v) \quad \forall a \in F, \quad \forall v \in X. \)

An isomorphism is a linear map that is bijective (1-1 and onto).
Example (of vector spaces):

(i) \( K^n := \{(a_1, \ldots, a_n) : a_i \in K\} \). Addition and multiplication are defined componentwise.

(ii) Set of Functions \( IR \rightarrow IR \) (with \( K = IR \)).

(iii) Set of Functions \( S \rightarrow K \) for an arbitrary set \( S \).

(iv) Set of polynomials of degree \( < n \), coefficients from \( K \).

Exercise: (i) is isomorphic to (iv), and to (iii) if \( |S| = n \).

Def: A subset \( Y \) of a vector space \( X \) is a \textit{subspace} if it too is a vector space.

Example (of subspaces; see previous example)

(i) \( Y = \{(0, a_2, \ldots, a_n, 0) : a_i \in K\} \subseteq K^n \)

(ii) \( Y = \{\text{functions with period } T \mid \pi \} \subseteq \{\text{functions } IR \rightarrow IR\} \)

(iii) \( Y = \{\text{constant functions} , S \rightarrow K\} \subseteq \{\text{functions} , S \rightarrow K\} \).

(iv) \( Y = \{a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n : a_i \in K\} \subseteq \{\text{polynomials of degree } < n\} \).

Def: If \( Y \) and \( Z \) are subsets of a vector space \( X \), then their 

\underline{sum} is \( Y + Z = \{y + z \mid y \in Y, z \in Z\} \), and their 

\underline{intersection} is \( Y \cap Z = \{x \mid x \in Y \text{ and } x \in Z\} \).

Prop: If \( Y \) and \( Z \) are subspaces of \( X \), then \( Y + Z \) and \( Y \cap Z \) are also subspaces.

Pf: Exercise. \( \square \)
Def: A linear combination of \( j \) vectors \( x_1, \ldots, x_j \) is a vector of the form \( a_1 x_1 + \cdots + a_j x_j \), \( a_i \in \mathbb{K} \).

Prop: The set of all linear combinations of \( x_1, \ldots, x_j \) is a subspace of \( \mathbb{K} \), and it is the smallest subspace of \( \mathbb{K} \) containing \( x_1, \ldots, x_j \).
(This is the subspace spanned by \( x_1, \ldots, x_j \), and denoted \( \langle x_1, \ldots, x_j \rangle \)).

Def: A set of vectors \( x_1, \ldots, x_m \in \mathbb{K} \) span \( \mathbb{K} \) if \( \mathbb{K} = \langle x_1, \ldots, x_j \rangle \).

Def: The vectors \( x_1, \ldots, x_j \) are linearly independent if we can write \( a_1 x_1 + \cdots + a_j x_j = 0 \), where not all \( a_i = 0 \). Otherwise, the vectors are linearly independent.

Lemma 1.1: Suppose that \( x_1, \ldots, x_n \) span \( \mathbb{K} \) and \( y_1, \ldots, y_j \in \mathbb{K} \) are linearly independent. Then \( j \leq n \).

Proof: Write \( y_1 = a_1 x_1 + \cdots + a_n x_n \), assume WLOG that \( a_1 \neq 0 \) (otherwise we may just renumber the \( x_i \)'s). Now, "solve" for \( x_1 \), i.e., write \( x_1 = b_1 y_1 + b_2 x_2 + \cdots + b_n x_n \).

We conclude that \( \langle y_1, x_2, \ldots, x_n \rangle = \mathbb{K} \).

Now, write \( y_2 = b_1 y_1 + b_2 x_2 + \cdots + b_n x_n \), assume WLOG that \( b_2 \neq 0 \).

Solve for \( x_2 \), i.e., write \( x_2 = c_1 y_1 + c_2 y_2 + c_3 x_3 + \cdots + c_n x_n \).

We conclude that \( \langle y_1, y_2, x_3, \ldots, x_n \rangle = \mathbb{K} \).

Continue in this manner. Note that \( j > n \) is impossible because \( y_1, \ldots, y_j \) are linearly independent. More precisely, if \( j > n \), then write \( y_j = a_1 y_1 + \cdots + a_n y_n \) (linear independence). \( \Box \)
Def: A set \( B \) of vectors that span \( X \) and are linearly independent is called a basis for \( X \).

Lemma 2: A vector space \( X \) which is spanned by a finite set of vectors \( x_1, \ldots, x_n \) has a finite basis, contained in this set.

Proof: If \( x_1, \ldots, x_n \) are linearly dependent, there is a nontrivial relation between them, so we can write \( x_n = a_1 x_1 + \ldots + a_{n-1} x_{n-1} \), and thus remove \( x_n \) from the set, i.e., \( x_1, \ldots, x_{n-1} \) spans \( X \). Repeat this process until the remaining set is linearly independent, and then it must be a basis.

Def: A vector space \( X \) is finite dimensional if it has a finite basis.

Examples: In \( \mathbb{R}^3 \), any two vectors that do not lie on the same line are linearly independent. They span a 2-dimensional subspace (a plane). Any three vectors are linearly independent if and only if they do not lie on the same plane.

In \( \mathbb{R}^2 \), if \( v \) and \( w \) are not scalar multiples, then \( \langle v, w \rangle = 1 \mathbb{R}^2 \); i.e., \( v, w \) forms a basis for \( \mathbb{R}^2 \). While there are many bases, we call \( e_1, e_2 \), where \( e_1 = (1,0) \), \( e_2 = (0,1) \) the standard unit basis vectors. These can be easily generalized to \( \mathbb{R}^n \) for any \( n \).
Theorem 1.3: All bases for a finite-dimensional vector space have the same cardinality, which we call the dimension of $X$, denoted $\dim X$.

Proof: Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$ be two bases for $X$. By Lemma 1.1, $m \leq n$ and $n \leq m \Rightarrow n = m$. \qed

Theorem 1.4: Every linear independent set of vectors $y_1, \ldots, y_j$ in a finite-dimensional vector space $X$ can be extended to a basis of $X$.

Proof: If $\langle y_1, \ldots, y_j \rangle \neq X$, then $\exists x \in X$ such that $x \notin \langle y_1, \ldots, y_j \rangle$. Add this to the $y_i$'s, and repeat the process. This will terminate in less than $n = \dim X$ steps, because otherwise $X$ would contain more than $n$ linearly independent vectors. \qed

Theorem 1.5: (a) Every subspace $Y$ of a finite-dimensional vector space $X$ is finite-dimensional.
(b) Every subspace $Y$ has a complement in $X$, that is, another subspace $Z$ (sometimes denoted $Y^\perp$) such that every vector $x \in X$ can be decomposed uniquely as $x = y + z$, $y \in Y$, $z \in Z$.

Furthermore, $\dim X = \dim Y + \dim Z$.

Proof: Pick $y_1 \in Y$, and extend this to a basis $y_1, \ldots, y_j$ of $Y$ (Theorem 1.4). By Lemma 1.1, $j \leq \dim X < \infty$.

By Theorem 1.4, we can extend this to a basis $y_1, \ldots, y_j, z_1, \ldots, z_n$ of $X$. Clearly, $Y$ and $Z$ are complements, and $\dim X = n = j + (n-j) = \dim Y + \dim Z$. \qed
Def: $X$ is the direct sum of subspaces $Y_1$ and $Z$ that are complements of each other. More generally, $X$ is the direct sum of subspaces $Y_1, \ldots, Y_m$ if every $x \in X$ can be expressed uniquely as $x = y_1 + \cdots + y_m$, $y_i \in Y_i$. We denote this as $X = Y_1 \oplus \cdots \oplus Y_m$.

Prop: If $\dim X < \infty$ and $X = Y_1 \oplus \cdots \oplus Y_m$, then $\dim X = \sum_{i=1}^{m} \dim Y_i$.

Proof: Exercise.

Def: An $(n-1)$-dimensional subspace of an $n$-dimensional space is called a hyperplane.

Example: Let $X = \mathbb{R}^3$, $Y = xy$-plane, $Z = \langle z \rangle$ where $z \notin Y$.

Then $X = Y \oplus Z$, and $Y$ is a hyperplane.

A direct sum is a way to "multiply" two spaces. We can also take a quotient, or "divide" a space by a subspace.

Def: If $Y$ is a subspace of $X$, then two vectors $x_1, x_2 \in X$ are congruent modulo $Y$, denoted $x_1 \equiv x_2 \mod Y$, if $x_1 - x_2 \in Y$.

Prop: Congruence mod $Y$ is an equivalence relation, i.e., it is

(i) symmetric: $x_1 \equiv x_2 \Rightarrow x_2 \equiv x_1$.

(ii) reflexive: $x \equiv x$ for all $x \in X$.

(iii) transitive: $x_1 \equiv x_2$ and $x_2 \equiv x_3 \Rightarrow x_1 \equiv x_3$.

Also, if $x_1 \equiv x_2$, then $ax_1 = ax_2$ for all $a \in K$.

Ref: Exercise.
The equivalence classes are called congruence classes mod $Y$. Denote the congruence class containing $x$ by $\{x\}$. (Also called cosets).

Example: Let $X = \mathbb{R}^3$, and $Y$ be any 1D subspace (line) and $Z$ be any 2D subspace. The congruence classes mod $Y$ are the lines parallel to $Y$, and the congruence classes mod $Z$ are the planes parallel to $Z$.

The set of congruence classes can be made into a vector space by defining addition and multiplication by scalars as follows:

$$\{x\} + \{z\} = \{x+z\} \quad \text{and} \quad a\{x\} = \{ax\}.$$ 

Prop: This addition and multiplication is well-defined, that is, it is independent of the choice of representatives of the congruence classes.

Def: The vector space of congruence classes defined above is called the quotient space of $X$ mod $Y$, denoted $X \mod Y$, or $X/Y$.

Example: Take $X = \mathbb{R}^n$ ($n \geq 3$) and $K = \mathbb{R}$, and let $Y = \{(0, 0, a_3, \ldots, a_n) : a_i \in \mathbb{R}\}$. Two vectors are congruent mod $Y$ iff their first $2$ components are equal. Each equivalence class can be represented as a pair $(a_1, a_2)$, so $X/Y$ is isomorphic to $\mathbb{R}^2$.

Think of $X/Y$ as "throwing away" info in the components that pertains to $Y$. 
Theorem 1.6: If \( Y \) is a subspace of a finite-dimensional vector space \( X \), then \( \dim Y + \dim (X/Y) = \dim X \).

\textbf{Pf: } Let \( y_1, \ldots, y_j \) be a basis for \( Y \). By Theorem 4, we can extend this to a basis \( y_1, \ldots, y_j, x_{j+1}, \ldots, x_n \) of \( X \).

\textbf{Claim: } \( \{x_{j+1}\}, \ldots, \{x_n\} \) is a basis of \( X/Y \).

\textbf{Pf: } (They span \( X/Y \)): Pick \( \{x_i\} \in X/Y \), and write
\[
X = \sum_{i=1}^{j} a_i y_i + \sum_{k=j+1}^{n} b_k x_k = \{x_i\} = \{ \Sigma a_i y_i + \Sigma b_k x_k \}
= \Sigma a_i \{y_i\} + \Sigma b_k \{x_k\} = \Sigma b_k \{x_k\}. \quad \checkmark
\]

(They are lin. indep): Suppose \( \sum_{i=j+1}^{n} c_k \{x_k\} = 0. \)

This means \( \Sigma c_k x_k = y_i \), for some \( y_i \in Y \).

Write \( y = \sum_{i=1}^{j} d_i y_i \Rightarrow \Sigma c_k x_k - \Sigma d_i y_i = 0. \)

Since \( y_1, \ldots, x_n \) is a basis of \( X \), all \( c_k, d_i = 0. \quad \checkmark \)

We conclude that \( \dim (X/Y) = \# \) of \( x_k = n - j \) and \( \dim Y + \dim X/Y = j + (n-j) = n = \dim X. \quad \checkmark \)

\textbf{Corollary: } If a subspace \( Y \) of a finite-dimensional vector space \( X \) has \( \dim Y = \dim X \), then \( Y = X. \)

\textbf{Pf: } Exercise.
Theorem 1.7 Let $U, V$ be subspaces of a finite-dimensional vector space $X$, with $U + V = X$. Then $\dim X = \dim U + \dim V - \dim (U \cap V)$.

Pf: Let $W = U \cap V$. Note that the case when $U \cap V = \{0\}$ is handled by Theorem 1.5.

Define $\overline{U} = U/W$, $\overline{V} = V/W$, and so $\overline{U} \cap \overline{V} = \{0\}$ and $\overline{X} = X/W$ satisfy $\overline{X} = \overline{U} + \overline{V}$.

By Theorem 5, $\dim \overline{X} = \dim \overline{U} + \dim \overline{V}$.

By Theorem 6, $\dim \overline{X} = \dim X - \dim W$
\[ \dim \overline{U} = \dim U - \dim W \]
\[ \dim \overline{V} = \dim V - \dim W. \]

Together, these imply:
\[ \dim \overline{X} = \dim \overline{U} + \dim \overline{V} \]
\[ (\dim X - \dim W) = (\dim U - \dim W) + (\dim V - \dim W) \]
\[ \Rightarrow \dim X = \dim U + \dim V - \dim W. \quad \square \]

Def: If $X_1, X_2$ are vector spaces over $K$, then their Cartesian sum is the set $\{(x_1, x_2) : x_1 \in X_1, x_2 \in X_2\}$, with addition and multiplication defined component-wise, denoted $X_1 \oplus X_2$.

Prop: $X_1 \oplus X_2$ is a linear space, and $\dim (X_1 \oplus X_2) = \dim X_1 + \dim X_2$.

Pf: Exercise.
An interesting example: let \( X \) be the set of all functions \( x(t) \) that satisfy \( \frac{d^2}{dt^2} x + x = 0 \).

If \( x_1(t), x_2(t) \) are solutions, then so are \( x_1(t) + x_2(t) \), and \( c x_1(t) \).

Thus \( X \) is a vector space.

Solutions describe the motion of a mass-spring system (simple harmonic motion). A particular solution is determined completely by specifying the initial position \( x(0) = p \), and initial velocity, \( x'(0) = v \).

Thus, we can describe an element \( x(t) \in X \) by a pair \((p, v)\), \( p, v \in \mathbb{R} \).

We can check that this defines an isomorphism

\[
X \rightarrow \mathbb{R}^2, \quad x(t) \mapsto (x(0), x'(0)).
\]

Note that \( \cos x \) and \( \sin x \) are two linearly independent solutions (not scalar multiples of each other). Thus, the general solution to this differential equation is

\[
C_1 \cos x + C_2 \sin x, \quad C_1, C_2 \in \mathbb{R}.
\]

Said differently, \( \{\cos x, \sin x\} \) is a basis for the solution space of \( x'' + x = 0 \).