MTHSC 853: Linear Algebra

1. Linear algebra fundamentals.

A group is a set G and associative binary operation $*$ with

- closure: $a, b \in G \Rightarrow a * b \in G$
- identity: $\exists\, e \in G$ such that $a * e = e * a = a \quad \forall a \in G$.
- inverses: $\forall a \in G$, $\exists\, b$ such that $a * b = b * a = e$.

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

Def: A field is a set F containing $1 \neq 0$ with two binary operations, $+$ (addition) and $\cdot$ (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: $a(b+c) = ab + ac \quad \forall a, b, c \in F$.

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 "compatable" in that they have natural associtative & 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) $(-1)x = -x$ 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) $\phi(av) = a\phi(v) \quad \forall a \in F, \forall v \in X.$

An __isomorphism__ is a linear map that is bijective (1-1 and onto).

<u>Examples</u> (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 $\mathbb{R} \to \mathbb{R}$ (with $K = \mathbb{R}$).

(iii) Set of functions $S \to K$ for an arbitrary set S.

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

<u>Exercise</u>: (i) is isomorphic to (iv), and to (iii) if $|S| = n$.

<u>Def</u>: A subset Y of a vector space X is a <u>subspace</u> if it too is a vector space.

<u>Examples</u> (of subspaces; see previous example)

(i) $Y = \{(0, a_2, \ldots, a_{n-1}, 0) : a_i \in K\} \subseteq K^n$

(ii) $Y = \{\text{functions with period } T | \pi\} \subseteq \{\text{functions } \mathbb{R} \to \mathbb{R}\}$

(iii) $Y = \{\text{constant functions } S \to K\} \subseteq \{\text{functions } S \to K\}$.

(iv) $Y = \{a_0 + a_2 x^2 + a_4 x^4 + \cdots + a_{n-1} x^{n-1} : a_i \in K\} \subseteq \{\text{polynomials of degree} < n\}$.

<u>Def</u>: If Y and Z are subsets of a vector space X, then their...

<u>sum</u> is $Y + Z = \{y + z \mid y \in Y, z \in Z\}$, and their

<u>intersection</u> is $Y \cap Z = \{x \mid x \in Y \text{ and } x \in Z\}$.

<u>Prop</u>: If Y and Z are subspaces of X, then $Y + Z$ and $Y \cap Z$ are also subspaces.

<u>Pf</u>: Exercise. $\square$

Def: A <u>linear combination</u> of j vectors $x_1, \dots, x_j$ is a vector of the form $a_1 x_1 + \dots + a_j x_j \quad a_i \in K$.

Prop: The set of all linear combinations of $x_1, \dots, x_j$ is a subspace of X, and it is the smallest subspace of X containing $x_1, \dots, x_j$. (This is the subspace <u>spanned</u> by $x_1, \dots, x_j$, and denoted $\langle x_1, \dots, x_j \rangle$).

Def: A set of vectors $x_1, \dots, x_m \in X$ <u>span</u> X if $X = \langle x_1, \dots, x_j \rangle$.

Def: The vectors $x_1, \dots, x_j$ are <u>linearly dependent</u> if we can write $a_1 x_1 + \dots + a_j x_j = 0$, where not all $a_i = 0$. Otherwise, the vectors are <u>linearly independent</u>.

Lemma 1.1: Suppose that $x_1, \dots, x_n$ span X and $y_1, \dots, y_j \in X$ are linearly independent. Then $j \leq n$.

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

We conclude that $\langle y_1, x_2, \dots, x_n \rangle = X$.

Now, write $y_2 = b_1 y_1 + b_2 x_2 + \dots + b_n x_n$, assume WLOG that $b_2 \neq 0$.

Solve for x_2, i.e, write $x_2 = c_1 y_1 + c_2 y_2 + c_3 x_3 + \dots + c_n x_n$.

We conclude that $\langle y_1, y_2, x_3, \dots, x_n \rangle = X$.

Continue in this manner. Note that $j > n$ is impossible because $y_1, \dots, y_j$ are linearly independent. More precisely, if $j > n$, then write $y_j = a_1' y_1 + \dots + a_n' y_n$ ↯ (linear independence). $\square$

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 $x_1, \dots, x_n$ has a finite basis, contained in this set.

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

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 $\langle v, w \rangle = \mathbb{R}^2$; 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.

<u>Theorem 1.3</u>: All bases for a finite-dimensional vector space have the same cardinality, which we call the <u>dimension</u> of X, denoted $\dim X$.

<u>Proof</u>: 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 $n \leq m \Rightarrow n = m$. $\square$

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

<u>Proof</u>: 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. $\square$

<u>Theorem 1.5</u>: (a) Every subspace Y of a finite-dimensional vector space X is finite-dimensional.

(b) Every subspace Y has a <u>complement</u> 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, $\dim X = \dim Y + \dim Z$.

<u>Proof</u>: 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 $y_1, \ldots, y_j, z_{j+1}, \ldots, z_n$ of X. Clearly, Y and Z are complements, and

$$\dim X = n = j + (n-j) = \dim Y + \dim Z.$$

$\square$

Def: X is the direct sum of subspaces Y and Z that are complements of each other. More generally, X is the direct sum of subspaces $Y_1, \dots, Y_m$ if every $x \in X$ can be expressed uniquely as $x = y_1 + \dots + y_m$, $y_i \in Y_i$. We denote this as $X = Y_1 \oplus \dots \oplus Y_m$.

Prop: If $\dim X < \infty$ and $X = Y_1 \oplus \dots \oplus Y_m$, 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 $x_1 \equiv x_2 \bmod Y$, 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 $a x_1 \equiv a x_2$ for all $a \in K$.

Pf: Exercise.

The equivalence classes are called <u>congruence classes</u> mod Y. Denote the congruence class containing x by $\{x\}$. (Also called <u>cosets</u>).

<u>Example</u>: 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 Y 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:

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

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

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

<u>Example</u>: 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.

<u>Theorem 1.6</u>: If Y is a subspace of a finite-dimensional vector space X, then $\dim Y + \dim(X/Y) = \dim X$.

<u>Pf</u>: Let $y_1, \dots, y_j$ be a basis for Y. By Theorem 4, we can extend this to a basis $y_1, \dots, y_j, x_{j+1}, \dots, x_n$ of X.

<u>Claim</u>: $\{x_{j+1}\}, \dots, \{x_n\}$ is a basis of X/Y.

<u>Pf</u>: • (They span X/Y): Pick $\{x\} \in X/Y$, and write

$$x = \sum_{i=1}^{j} a_i y_i + \sum_{k=j+1}^{n} b_k x_k \Rightarrow \{x\} = \{ \Sigma a_i y_i + \Sigma b_k x_k \}$$

$$= \Sigma a_i \{y_i\} + \Sigma b_k \{x_k\} = \Sigma b_k \{x_k\}. \quad \checkmark$$

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

This means $\Sigma c_k x_k = y$, for some $y \in Y$.

write $y = \sum_{i=1}^{j} d_i y_i \Rightarrow \Sigma c_k x_k - \Sigma d_i y_i = 0$.

Since $y_1, \dots, x_n$ is a basis of X, all $c_k, d_i = 0$. ✓

We conclude that $\dim(X/Y) = \#$ of $x_k = n-j$

and $\dim Y + \dim X/Y = j + (n-j) = n = \dim X$. □

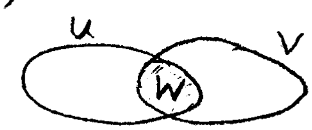
<u>Corollary</u>: If a subspace Y of a finite-dimensional vector space X has $\dim Y = \dim X$, then $Y = X$.

<u>Pf</u>: 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 $\bar{U} = U/W$, $\bar{V} = V/W$, and so $\bar{U}\cap\bar{V} = \{0\}$ and $\bar{X} := X/W$ satisfies $\bar{X} = \bar{U}+\bar{V}$.



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

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

Together, these imply:
$$\dim \bar{X} = \dim \bar{U} + \dim \bar{V}$$
$$(\dim X - \dim W) = (\dim U - \dim W) + (\dim V - \dim W)$$
$$\Rightarrow \quad \dim X = \dim U + \dim V - \dim W. \qquad \square$$

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 componentwise, 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.

<u>An interesting example</u>: 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), $\quad p, v \in \mathbb{R}$.

We can check that this defines an isomorphism

$$X \longrightarrow \mathbb{R}^2, \qquad x(t) \longmapsto (x(0),\ x'(0)).$$

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

$$C_1 \cos x + C_2 \sin x, \qquad C_1, C_2 \in \mathbb{R}.$$

Said differently, $\{\cos x, \sin x\}$ is a <u>basis</u> for the solution space of $x'' + x = 0$.