MTHSC 853: Linear Algebra

1. Linear algebra fundamentals.

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

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

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

* 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.

<u>Prop</u>: In <u>any</u> vector space X,

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

<u>Pf</u>: Exercise (easy). $\square$

<u>Def</u>: A <u>linear map</u> 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 <u>isomorphism</u> is a linear map that is bijective (1-1 and onto).

Examples (of vector spaces):

(i) $K^n := \{(a_1, \dots, a_n) : a_i \in K\}$. 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.

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

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

Examples (of subspaces; see previous example)

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

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

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

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

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. $\square$

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

<u>Prop</u>: 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 $\langle x_1, \dots, x_j \rangle$).

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

<u>Def</u>: 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>.

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

<u>Proof</u>: 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 $y_j = a_1' y_1 + \dots + a_n' y_n$ $\lightning$ (linear independence). $\square$

Def A set B of vectors that span X and are linearly independent is called a <u>basis</u> for X.

<u>Lemma 2</u>: 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.

Pf: If $x_1, \ldots, x_n$ are linearly dependent, there is a nontrivial relation between them; so we can write $x_n = a_1 x_1 + \cdots + a_{n-1} x_n$, 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. $\square$

Def: A vector space X is <u>finite dimensional</u> if it has a finite basis.

<u>Examples</u>: In $\mathbb{R}^3$, any two vectors that do <u>not</u> 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 <u>not</u> 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 <u>many</u> bases, we call e_1, e_2, where $e_1 = (1,0)$, $e_2 = (0,1)$ the <u>standard unit basis vectors</u>. 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 $x_1, \dots, x_n$ and $y_1, \dots, y_m$ be two bases for X. By lemma 1.1, $m \le n$ and $n \le m \Rightarrow n = m$. □

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

Proof: If $\langle y_1, \dots, y_j \rangle \neq X$, then $\exists\, x \in X$ such that $x \notin \langle y_1, \dots, y_j \rangle$. 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. □

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 $y_1, \dots, y_j$ of Y (Theorem 1.4.) By lemma 1.1, $j \le \dim X < \infty$. ✓

By Theorem 1.4, we can extend this to a basis $y_1, \dots y_j, z_{j+1}, \dots, z_n$ of X. Clearly, Y and Z are complements, and

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

□

Def: X is the <u>direct sum</u> of subspaces Y & 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 $X = Y_1 \oplus \cdots \oplus Y_m$.

Def: If X_1, X_2 are vector spaces over K, then their <u>direct product</u> is $X_1 \times X_2 := \{(x_1, x_2) : x_1 \in X_1,\ x_2 \in X_2\}$, with addition & multiplication defined componentwise.

Prop: $\dim(Y_1 \oplus \cdots \oplus Y_m) = \sum_{i=1}^{m} \dim Y_m$

$\dim(X_1 \times \cdots \times X_m) = \sum_{i=1}^{m} \dim X_m$ (assume everything fin. dim'l.)

Ex: $X = \mathbb{R}^4$, $Y_1 = \{(a,b,0,0) : a,b \in \mathbb{R}\}$

$Y_2 = \{(0,0,c,d) : c,d \in \mathbb{R}\}$.

Clearly, $X = Y_1 \oplus Y_2$ since $(a,b,c,d) \overset{\text{uniquely.}}{=} (a,b,0,0) + (0,0,c,d)$

Ex: $X_1 = \mathbb{R}^2$, $X_2 = \mathbb{R}^2$.

$X_1 \times X_2 = \{((a,b),(c,d)) : (a,b) \in \mathbb{R}^2, (c,d) \in \mathbb{R}^2\} \simeq \{(a,b,c,d) : a,b,c,d \in \mathbb{R}\} = \mathbb{R}^4$.

So, for finite sums vs. products, there is no difference (up to isomorp.)

Ex: Let $X = \mathbb{R}^\infty = \{(a_1, a_2, a_3, \dots) : a_i \in \mathbb{R}\}$.

$$\simeq \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \dots$$

Let $X_1 = \{(a_1, 0, 0, \dots) : a_1 \in \mathbb{R}\}$

$X_2 = \{(0, a_2, 0, 0, \dots) : a_2 \in \mathbb{R}\}$

$\vdots$

Elements in the subspace $X_1 \oplus X_2 \oplus X_3 \oplus \dots$ are finite sums

$$x = x_{i_1} + x_{i_2} + \dots + x_{i_k}, \quad x_{i_j} \in X_{i_j}.$$

Thus, $X_1 \oplus X_2 \oplus X_3 \oplus \dots = \{(a_1, a_2, \dots, a_k, 0, 0, \dots) : a_i \in \mathbb{R},\ k \in \mathbb{Z}\}$.

$$\subsetneq \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \dots$$

Sums & products "multiply" spaces. We can also "divide" subspaces.

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: $x_1 \equiv x_2 \Rightarrow x_2 \equiv x_1$

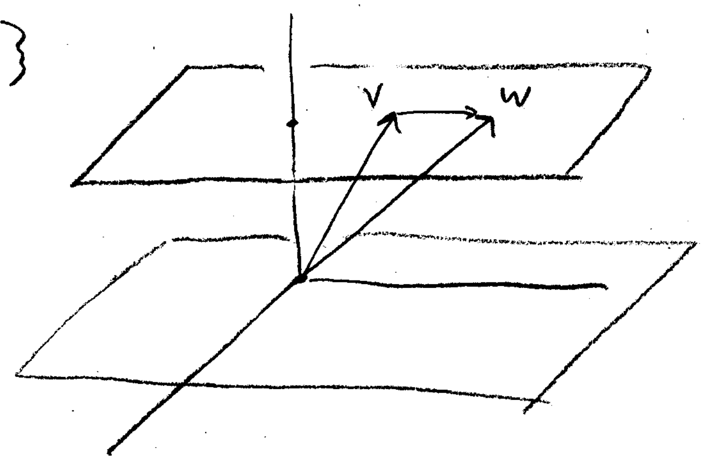
(ii) reflexive: $x \equiv x$ for all $x \in X$

(iii) transitive: $x \equiv y$ & $y \equiv z \Rightarrow x \equiv z$.

Also, if $x_1 \equiv x_2$, then $ax_1 \equiv ax_2$, all $a \in K$. (Exercise)

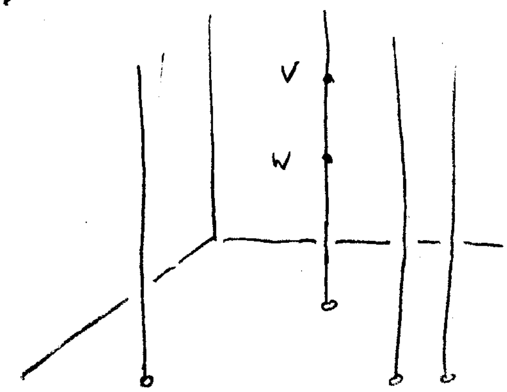
The equivalence classes are called <u>congruence classes</u> mod Y, or <u>cosets</u>. Denote the class containing x by $\{x\}$.

<u>Ex</u>: $X = \mathbb{R}^3$, $Y = \{(x,y,0) : x,y \in \mathbb{R}\}$
$= xy$-plane.



Then $v \equiv w \mod Y$ if they lie on the same horizontal plane.

<u>Ex</u>: $X = \mathbb{R}^3$, $Z = \{(0,0,z) : z \in \mathbb{R}\}$
$= z$-axis.



Then $v \equiv w \mod Z$ if they lie on the same vertical line.

Let X/Y denote the set of equivalence classes mod Y.

This can be made into a vector space by defining addition & scalar multiplication as follows.

$$\{x\} + \{z\} = \{x+z\}, \qquad a\{x\} = \{ax\}.$$

Need to check this is <u>well-defined</u>, that is, it is independent of the choice of representation from the classes. (Exercise)

This vector space X/Y is called the <u>quotient space</u> of X mod Y.

<u>Theorem 1.6</u>: If Y is a subspace of a finite-dim'l 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 1.4, 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> • <u>Spans</u> X/Y: Pick $\{x\}$ in X/Y, write

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

$$= \sum a_i \{y_i\} + \sum b_k \{x_k\} = \sum b_k \{x_k\} \checkmark$$

• <u>Lin. indep</u>: Suppose $\sum_{i=j+1}^{n} c_k \{x_k\} = \{0\}$.

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

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

Since $y_1, \dots, y_j, x_{j+1}, \dots, x_n$ is a basis for X, all $c_k, d_i = 0$ ✓

Thus, $\dim(X/Y) = n-j$, $\dim Y = j$, $\dim X = j + (n-j) = n$. ◻

<u>Cor</u>: If a subspace Y of a fin. dim'l vector space X has $\dim Y = \dim X$, then $Y = X$. (<u>Exercise</u>)

<u>Theorem 1.7</u>: Let U, V be subspaces of a fin. dim'l space X, with $U+V=X$. Then $\dim X = \dim U + \dim V - \dim(U \cap V)$.

<u>Pf</u>: Let $W = U \cap V$. Note that the case of $W = \{0\}$ is covered by Thm. 1.5.

Define $\bar{U} = U/W$, $\bar{V} = V/W$, so $\bar{U} \cap \bar{V} = \{0\}$, $\bar{X} := X/W$ satisfies $\bar{X} = \bar{U} + \bar{V}$.

By Thm 1.6,
$$\dim \bar{X} = \dim X + \dim W$$
$$\dim \bar{U} = \dim U - \dim W$$
$$\dim \bar{V} = \dim V - \dim W.$$

By Thm 1.5, $\dim \bar{X} = \dim \bar{U} + \dim \bar{V}$

$$\Rightarrow (\dim X - \dim W) = (\dim U - \dim W) + (\dim V - \dim W)$$

$$\Rightarrow \dim X = \dim U + \dim V - \dim V. \qquad \square$$

<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 sol'ns, then so are $x_1(t)$, $x_2(t)$, & $c\,x_1(t)$

Thus, X is a vector space.

Solutions describe the motion of a mass-spring system (simple harmonic motion). A particular sol'n 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), $p, v \in \mathbb{R}$.

<u>Check</u>: This defines an isomorphism

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

Note that $\cos x$ & $\sin x$ are two linearly independent solutions $(a \cos x + b \sin x = 0 \Rightarrow a = b = 0.)$ Thus, the <u>general solution</u> to this differential equation is

$a \cos x + b \sin x$, $\quad a, b \in \mathbb{R}$.

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

<u>Remark</u>. $\cos x + i \sin x = e^{ix}$, $\quad \cos x - i \sin x = e^{-ix}$,

so $\{e^{ix}, e^{-ix}\}$ is another basis!

So we could write $C_1 e^{ix} + C_2 e^{-ix}$, instead.