# MATH 350 Linear Algebra
# Exam 1 Review Notes

Instructor: Will Chen

October 6, 2022

Here is a **non-comprehensive** overview of what we have covered. You should make sure you are familiar with these topics. Unless otherwise stated, you should be able to recite all definitions. You should be able to prove every theorem we've covered. As an exercise, when reading each theorem below, try to remember how it was proved. You should be able to answer all of the questions I pose below, and give justifications/proofs when relevant.
**Caution:** There are probably typos. If you think you've found one, please lmk ASAP! If you find a typo/mistake that could potentially cause mathematical confusion, you will receive **a bonus point on the exam.**

## 1 Vector spaces, subspaces, and quotient spaces

**Definition 1** (Vector space, abridged)**.** A vector space over a field $F$ is a set $V$ together with two operations $+ : V \times V \to V$ and $\cdot : F \times V \to V$ which satisfies the properties VS1-VS8 (see §1.2 in the book).

An element of a vector space is called a vector. We sometimes leave out the field $F$, and simply say "let $V$ be a vector space". In this case it should be understood that $V$ is a vector space over some field $F$. If we write "Let $V, W$ be vector spaces", then it should be understood that they are vector spaces over the same field. You should know the definition of a field, but you do not need to memorize it for this exam.

**Definition 2** (Fields)**.** A field $F$ is a set with two operations $+ : F \times F \to F$ and $\cdot : F \times F \to F$, such that the following hold for all $a, b, c \in F$:

(F1) $a + b = b + a$ and $a \cdot b = b \cdot a$

(F2) $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(F3) There exist distinct elements "0" and "1" in $F$ such that

$$0 + a = a \quad \text{and} \quad 1 \cdot a = a$$

(F4) For each $a \in F$ and *nonzero* $b \in F$, there exist elements $c, d \in F$ such that

$$a + c = 0 \quad \text{and} \quad b \cdot d = 1$$

Here, $c$ is called the negative of $a$, denoted "$-a$", and $d$ is called the multiplicative inverse of $b$, denoted "$b^{-1}$" or "$1/b$".

(F5) $a \cdot (b + c) = a \cdot b + a \cdot c$

**Definition 3** (Subspace)**.** A subspace of a vector space $V$ is a subset $W \subset V$ satisfying:

(a) $0 \in W$

(b) For any $x, y \in W$, $x + y \in W$.

(c) For any $x \in W, a \in F$, $ax \in W$.

Recall that $A \subset B$ means $A$ is a subset of $B$. This does not rule out the case $A = B$. If we want to say that $A$ is a proper subset of $B$, we will write $A \subsetneq B$.

In class I mistakenly noted that the last two conditions in the definition imply the first. They do not! For example, the empty subset $\{\} \subset V$ satisfies the last two conditions, but does not satisfy the first. All three conditions are required!

As the course progresses you should be collecting a list of examples to refer to. For example, we have discussed $F^n$ (where $F$ is a field), spaces of functions (all functions, linear functions, continuous functions...etc), spaces of polynomials "$P_n(F)$" and "$P(F)$", spaces of $m \times n$ matrices...

Have an understanding of basic properties of subspaces of a vector space $V$.

- How many 0-dimensional subspaces are there?
- If $\dim V = n$, how many $n$-dimensional subspaces are there?
- What are the 1-dimensional subspaces in $F^n$?
- Is the intersection of 2 subspaces a subspace?
- Is the intersection of arbitrarily many subspaces a subspace?
- If $W_1, W_2 \subset V$ are subspaces, what is $W_1 + W_2$? What does $W_1 \oplus W_2$ mean? Are they subspaces?
- What are other ways of constructing subspaces?

You should be able to answer the questions above and give justifications when relevant.

Recall the definition of quotient spaces (also called coset spaces)

**Definition 4.** Let $V$ be a vector space and $W \subset V$ a subspace. If $v \in V$, then

$$v + W := \{v + w \mid w \in W\}$$

is called the *coset of* $W$ *containing* $v$. The *quotient space* $V/W$ is defined to be the set

$$V/W := \{v + W \mid v \in V\}$$

equipped with the operations of addition and scalar multiplication:

$$(v + W) + (v' + W) = (v + v') + W \qquad a(v + W) = (av) + W \qquad \text{for all } v, v' \in V, a \in F$$

We showed in the homeworks that these operations are well defined and make $V/W$ into a vector space.

- If $v, v' \in V$, when is $v + W = v' + W$? If $v \neq v'$, must $v + W \neq v' + W$?
- If $v + W \neq v' + W$, what is $(v + W) \cap (v' + W)$?
- If $(v + W) \cap (v' + W)$ is nonempty, must $v + W = v' + W$?

## 2 Linear combination, span and linear independence

**Definition 5** (Linear combination)**.** If $V$ is a vector space and $S \subset V$ a subset, then a linear combination of vectors in $S$ is a vector of the form

$$a_1 s_1 + a_2 s_2 + \cdots + a_n s_n$$

for some collection of scalars $a_i \in F$ and $s_i \in S$.

**Definition 6** (Span)**.** If $V$ is a vector space and $S \subset V$ a subset, then $\text{Span}(S)$ is the set of all linear combinations of vectors in $S$. We say that $S$ spans $V$ (or $S$ generates $V$, or $S$ is a spanning set for $V$) if $\text{Span}(S) = V$.

Note that $S$ doesn't have to be finite!

- What is the relationship between $S, \text{Span}(S), V$?
- What is $\text{Span}(V)$?

The following alternate characterization of span is often useful:

**Theorem 7.** *If $V$ is a vector space and $S \subset V$ a subset, then* $\text{Span}(S)$ *is the intersection of all subspaces containing $S$.*

The slogan here is that "$\text{Span}(S)$ is the smallest subspace containing $S$". Here, by "slogan" I mean a phrase which is not precise, but is easy to remember and conveys the right intuition.

(a) What is not precise about the statement "$\text{Span}(S)$ is the smallest subspace containing $S$"?

The concepts of span and linear independence are "dual" to each other. This is a philosophy to keep in mind. Whenever you see a theorem about one, think about what the corresponding statement would be for the other. Here are some examples:

**Theorem 8** (Existence vs uniqueness)**.** *Let $S$ be a subset of a vector space $V$. Then*

*(a) $S$ spans $V$ if and only if every $v \in V$ is a linear combination of vectors in $S$.*

*(b) $S$ is linearly independent if and only if any $v \in V$ which is a linear combination of vectors in $S$ is a linear combination of vectors in $S$ in a* unique way*.*

The moral here is that span is essentially about "existence", whereas linear independence is about "uniqueness".

**Theorem 9** (Permanence under subset vs superset)**.** *Let $S$ be a subset of a vector space $V$. Then*

*(a) If $S$ spans $V$, and $S' \supset S$, then $S'$ also spans $V$..*

*(b) If $S$ is linearly independent and $S' \subset S$, then $S'$ is also linearly independent.*

The slogan is: "supersets of spanning sets are also spanning", and "subsets of linearly independent sets are also linearly independent".

**Theorem 10** (Linear independence in terms of span)**.** *Let $S$ be a subset of a vector space $V$, then $S$ is linearly independent if and only if no element $s \in S$ is in the span of $S - \{s\}$.*

Here, the "dual" statement to the above can be considered to be itself.

# 3 Bases and dimension

The notions of basis and dimension go hand in hand.

**Definition 11** (Basis)**.** A basis of a vector space $V$ is a subset $S \subset V$ that is linearly independent and spans $V$.

The plural of basis is "bases". Know the replacement theorem:

**Theorem 12** (Replacement theorem, Theorem 1.10 in the book)**.** *Let $V$ be a vector space that is generated by a set $G$ of size $n$. Let $L$ be a linearly independent subset of $V$ of size $m$. Then $m \leq n$, and there exists a subset $H$ of $G$ containing exactly $n - m$ vectors such that $L \cup H$ generates $V$.*

It follows from the replacement theorem that

**Theorem 13** (All bases have the same size)**.** *Let $V$ be a vector space with a finite spanning set. Then $V$ has a finite basis, and any two bases for $V$ have the same size.*

You should know how to prove this using the replacement theorem. Because of the theorem, the following definition makes sense:

**Definition 14** (Dimension)**.** Let $V$ be a vector space. If $V$ has a finite spanning set, then the dimension of $V$ is defined to be the size of any basis. If $V$ doesn't have a finite spanning set, then its dimension is infinite.

You should know the two alternate characterizations of a basis:

**Theorem 15.** *Let $V$ be a vector space.*

*(a) A subset $S \subset V$ is a basis if and only if it is a minimal spanning set. In other words, $S$ is a basis if and only if $S$ spans $V$ and any strict subset $S' \subsetneq S$ does not span $V$.*

*(b) A subset $S \subset V$ is a basis if and only if it is a maximal linearly independent set. In other words, $S$ is linearly independent, and any strict superset $S' \supsetneq S$ is not linearly independent.*

Slogan: A basis is a minimal spanning set. It is also a maximal linearly independent set.

If $V$ is finite dimensional, then we have the following numerical criterion for a set to be a basis:

**Theorem 16.** *Let $V$ be a vector space of dimension $n$. Then*

*(a) A subset $S \subset V$ is a basis if and only if $S$ is linearly independent and $|S| = n$.*

*(b) A subset $S \subset V$ is a basis if and only if $S$ spans $V$ and $|S| = n$.*

Some questions:

- If $V$ is an $n$-dimensional vector space. What are the possible sizes of linearly independent sets?
- If $V$ is an $n$-dimensional vector space. What are the possible sizes of spanning sets?
- If $W \subset V$ is a subspace, what is the relation between $\dim W$ and $\dim V$?
- If $S \subset V$ is linearly independent, does there exist a basis for $V$ that contains $S$? (I.e., can every linearly independent set be extended to a basis?)
- If $S \subset V$ is a basis, and $W \subset V$ a subset, must there exist a subset $S' \subset S$ such that $S'$ is a basis for $W$?
- If $S \subset V$ spans $V$, must there exist $S' \subset S$ such that $S'$ is a basis for $V$?
- If $S \subset V$ is linearly independent, is it a basis for a subspace of $V$?
- If $S \subset V$ spans $V$, is it a basis for a subspace of $V$?
- If $\mathbb{F}_p$ denotes a finite field with $p$ elements and $V$ is an $n$-dimensional vector space over $\mathbb{F}_p$, how many vectors are in $V$?

You should know the following theorem (i.e., know that it is true), but you do not need to know the proof (the proof basically involves the axiom of choice).

**Theorem 17.** *Every vector space has a maximal linearly independent set.*

- Does every vector space have a basis?

# 4 Linear transformations

**Definition 18.** A linear transformation is a function between vector spaces $f : V \to W$ such that

(a) For any $v, v' \in V$, $f(v + v') = f(v) + f(v')$, and

(b) For any $v \in V$, $a \in F$, $f(av) = af(v)$.

Sometimes for short we will simply say that $f : V \to W$ is *linear*. You should know that these properties imply that

$$f(a_1v_1 + a_2v_2 + \cdots + a_nv_n) = a_1f(v_1) + a_2f(v_2) + \cdots + a_nf(v_n)$$

for any $a_1, \ldots, a_n \in F$ and $v_1, \ldots, v_n \in F$. You should know how to prove this from the definition using induction.

As the course progresses, you should keep in mind a collection of examples of linear transformations. For example, differentiation, integration, rotation in $\mathbb{R}^2$, projection, reflection... There is also the zero linear transformation, and the identity linear transformation. Moreover, you can build linear transformations by adding linear transformations or multiplying by scalars. In other words,

**Theorem 19.** *Let $V, W$ be vector spaces. The set of all linear transformations $V \to W$ is denoted $\mathcal{L}(V, W)$. Then $\mathcal{L}(V, W)$ is a vector space with the operations of addition and scalar multiplication.*

**Definition 20.** Let $f : V \to W$ be a linear transformation. The image of $f$, denoted $\operatorname{im}(f)$ and the kernel of $f$, denoted $\ker(f)$ are:

$$\begin{aligned} \operatorname{im}(f) &:= \{f(v) \mid v \in V\} = \{w \in W \mid w = f(v) \text{ for some } v \in V\} \\ \ker(f) &:= \{v \in V \mid f(v) = 0\} \end{aligned}$$

The image is also sometimes called the *range*. The kernel is sometimes also called the *nullspace*.

**Theorem 21.** *Let $f : V \to W$ be a linear transformation. Then $\operatorname{im}(f)$ is a subspace of $W$, and $\ker(f)$ is a subspace of $V$.*

**Theorem 22** (Spans and linear transformations)**.** *Let $f : V \to W$ be a linear transformation. If $S \subset V$ spans $V$, then $f(S) := \{f(s) \mid s \in S\}$ spans $\operatorname{im}(f)$.*

**Definition 23.** The rank and nullity of $f$ are defined as:

$$\begin{aligned} \operatorname{rank}(f) &:= \dim \operatorname{im}(f) \\ \operatorname{nullity}(f) &:= \dim \ker(f) \end{aligned}$$

Sometimes this is infinite.

When the domain $V$ is finite dimensional, rank and nullity are finite and satisfy the

**Theorem 24** (Dimension theorem, Theorem 2.3 in the book)**.** *Let $f : V \to W$ be linear. If $V$ is finite dimensional, then*

$$\operatorname{rank}(f) + \operatorname{nullity}(f) = \dim(V)$$

- What happens if $V$ is infinite dimensional? If $V$ is infinite dimensional, could $\operatorname{rank}(f)$ and $\operatorname{nullity}(f)$ both be finite?

For linear transformations, we have the following useful characterizations of 1-1 and onto:

**Theorem 25.** *Let $f : V \to W$ be linear. Then*

*(a) $f$ is 1-1 if and only if $\ker(f) = 0$*

*(b) $f$ is onto if and only if $\operatorname{rank}(f) = \dim W$.*

A synonym for 1-1 is "injective". A synonym for onto is "surjective".

**Theorem 26.** *Let $f : V \to W$ be linear.*

*(a) If $f$ is injective, then for any linearly independent set $S \subset V$, $f(S)$ is also linearly independent. (Slogan: "$f$ injective implies that $f$ preserves linear independence")*

*(b) If $f$ is surjective, then for any spanning set $S \subset V$, $f(S)$ also spans $W$. (Slogan: "$f$ surjective implies that $f$ preserves spanning sets")*

More food for thought:

- Let $W \subset V$ be a subspace. Consider the map $p : V \to V/W$ defined by sending $v \mapsto v + W$. Is $p$ linear? What is $\ker(p)$? What is $\text{rank}(p)$? Is $p$ surjective? injective?

The following theorem is crucially important for understanding the relation between matrices and linear transformations:

**Theorem 27** (Theorem 2.6 in the book)**.** *Let $V, W$ be vector spaces. Let $v_1, \ldots, v_n$ be a basis for $V$. Let $w_1, \ldots, w_n$ be arbitrary elements of $W$. Then there exists exactly one linear transformation $f : V \to W$ such that $T(v_i) = w_i$ for each $i$.*

In the theorem, the fact that there is at least one such $f$ is due to $\{v_1, \ldots, v_n\}$ being linearly independent. The fact that there is at most one such $f$ is due to $\{v_1, \ldots, v_n\}$ being a spanning set for $V$. Since $\{v_1, \ldots, v_n\}$ is a basis, it is both linearly independent and spanning, so there is a unique such $f$.

# 5 Matrices and linear transformations

Let $V, W$ be vector spaces, and $\beta = (v_1, \ldots, v_n)$ an ordered basis for $V$. Recall that if $A$ is a set and $n \geq 1$ an integer, then $A^n$ denotes the $n$-fold cartesian product, whose elements are $n$-tuples $(a_1, \ldots, a_n)$ with each $a_i \in A$. If $|A| = m$, then $|A^n| = mn$.

Consider the map

$$\begin{array}{rcl} \Phi_\beta : \mathcal{L}(V, W) & \longrightarrow & W^n \\ f & \mapsto & (f(v_1), f(v_2), \ldots, f(v_n)) \end{array}$$

Theorem 27 implies:

**Theorem 28.** *The map $\Phi_\beta$ is a bijection (i.e., it is both 1-1 and onto).*

If $\gamma = (w_1, \ldots, w_m)$ is an ordered basis for $W$, then any $w \in W$ can be written as a linear combination of the $w_i$'s *in a unique way.* I.e, for any $w \in W$, there exist uniquely determined coefficients $a_1, \ldots, a_m$ such that $w = a_1 w_1 + a_2 w_2 + \cdots + a_m w_m$. This tuple of coefficients is often viewed as an $m \times 1$ matrix, called the *coordinate vector of $w$ relative to $\gamma$*, denoted

$$[w]_\gamma := \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix}$$

Let us write $([w]_\gamma)_i$ for the $i$th entry. In our notation above, we have $([w]_\gamma)_i = a_i$. Consider the map

$$\begin{array}{rcl} \Psi_\gamma : W^n & \longrightarrow & M_{m \times n}(F) \\ (x_1, \ldots, x_n) & \mapsto & A_{ij} \end{array}$$

where $A_{ij} := ([x_j]_\gamma)_i$. Then

**Theorem 29.** *The map $\Psi_\gamma$ is a bijection.*

Composing $\Phi_\beta$ and $\Psi_\gamma$, we have

**Theorem 30** (The matrix associated to a linear transformation)**.** *Let $V, W$ be vector spaces. Let $\beta = (v_1, \ldots, v_n)$ be an ordered basis for $V$, $\gamma = (w_1, \ldots, w_m)$ an ordered basis for $W$. Then the map*

$$\Psi_\gamma \circ \Phi_\beta : \mathcal{L}(V, W) \longrightarrow M_{m\times n}(F)$$

*is a bijective linear transformation. If $f \in \mathcal{L}(V, W)$, then the matrix of $f$ relative to the bases $\beta, \gamma$ is denoted*

$$[f]^\gamma_\beta := \Psi_\gamma(\Phi_\beta(f))$$

You should understand this map. Note that $\Psi_\gamma \circ \Phi_\beta$ is also *linear*. You should be able to compute the matrix of a linear transformation (relative to bases of the domain and codomain). Given a matrix $A$, you should also be able to find a linear transformation whose matrix is $A$ (relative to suitable bases).

**Caution:** Given a linear transformation $f : V \to W$, it does not make sense to speak of the matrix of $f$. To talk about the matrix of $f$, you need to choose a basis for $V$ and a basis for $W$. Any two bases will do, and relative to any two choses bases, you can compute a matrix for $f$. The matrix will usually depend on the chosen bases. Similarly, given a matrix $A$, to define a linear transformation whose matrix is $A$, one needs to choose vector spaces $V, W$ and appropriate bases for them. If $A$ is $m \times n$, then a convenient choice is to choose $V = F^n, W = F^m$, and to choose the bases to be the standard bases.

- Can you give an example that shows that the matrix of a linear transformation depends on the choice of bases $\beta, \gamma$?

If $f : V \to W$ and $g : W \to Z$ are linear maps between vector spaces, then the composition $g \circ f$ is the map

$$\begin{array}{rccc} g \circ f : V & \longrightarrow & Z \\ v & \mapsto & g(f(v)) \end{array}$$

Note that you can only compose if the codomain of the first map matches the domain of the second.

**Theorem 31.** *With notation as above, $g \circ f$ is linear.*

Some basic properties of composition are as follows. All are easily proven from the definitions.

**Theorem 32** (See Theorem 2.10 in the book for a more precise, but also more restrictive statement)**.** *Let $f, g, h$ be linear transformations (between possibly lots of different vector spaces). Let* id *denote the identity linear transformation (of some vector space). Whenever composition makes sense, we have*

*(a)* $f \circ (g + h) = f \circ g + f \circ h \quad$ *and* $\quad (g + h) \circ f = g \circ f + h \circ f$

*(b)* $f \circ (g \circ h) = (f \circ g) \circ h$

*(c)* $f \circ \mathrm{id} = \mathrm{id} \circ f = f$

*(d)* $a(f \circ g) = (af) \circ g = f \circ (ag)$ *for any scalar $a \in F$.*

The fact that $\Psi_\gamma \circ \Phi_\beta$ is linear tells us that addition and scalar multiplication of linear transformations corresponds to addition and scalar multiplication of matrices. The next natural question is: what does composition of linear transformations correspond to in terms of matrices? In other words, if $\alpha, \beta, \gamma$ are bases for $V, W, Z$ respectively, and $f : V \to W$, $g : W \to Z$ are linear, then what is the matrix $[g \circ f]^\gamma_\alpha$ in terms of $f, g$? The answer is:

**Theorem 33** (Composition corresponds to matrix multiplication, Theorem 2.11 in the book)**.** *Let $V, W, Z$ be finite dimensional vector spaces and let $f : V \to W$ and $g : W \to Z$ be linear transformations. Let $\alpha, \beta, \gamma$ be bases of $V, W, Z$ respectively. Then*

$$[g \circ f]^\gamma_\alpha = [g]^\gamma_\beta [f]^\beta_\alpha$$

*where the right hand side is the product of matrices.*

Note that $[g]_\beta^\gamma, [f]_\alpha^\beta$ will generally have different sizes. Indeed, if $\dim V = n, \dim W = m, \dim Z = r$, then $[g]_\beta^\gamma$ will be $r \times m$, $[f]_\alpha^\beta$ will be $m \times n$, and $[g \circ f]_\beta^\gamma$ will be $r \times n$. You should know how to multiply matrices.

We did not discuss this final theorem in class, but the proof is quite short. It is a good exercise to try to prove it.

**Theorem 34** (Theorem 2.14 in the book)**.** *Let $V, W$ be finite dimensional vector spaces having ordered bases $\beta$ and $\gamma$ respectively. Let $f : V \to W$ be linear. Then for each $v \in V$, we have*

$$[f(v)]_\gamma = [f]_\beta^\gamma [v]_\beta.$$

*Here, recall that $[f(v)]_\gamma$, $[v]_\beta$ are the coordinate vectors of $f(v)$ and $v$ with respect to $\gamma$ and $\beta$ respectively.*

Food for thought:

- Let $A$ be an $m \times n$ matrix and $B$ an $n \times p$ matrix. Let $(AB)_{*j}$ denote the $j$th column of $AB$. Does $(AB)_{*j}$ depend on every entry of the matrix $B$? Which entries does it depend on?
- Let $A$ be an $m \times n$ matrix and $B$ an $n \times p$ matrix. Let $B_{*j}$ denote the $j$th column of $B$. Can you write $B_{*j}$ as $BC$ for some matrix $C$? (Hint: By considering sizes of the matrices, $C$ would have to be a $p \times 1$ matrix)