

MAT224 Linear Algebra
Definitions, Lemmas, Theorems, Corollaries
and their related proofs

Tingfeng Xia

Winter 2019

by Tingfeng Xia

Materials in this booklet are based heavily on Prof. Nicolas Hoell's lectures as well as A COURSE IN LINEAR ALGEBRA by David B. Damiano and John B. Little.

Items in this booklet are, in fact, very similar to those in the book and are intended to be used as a bullet point guide to (almost) all the knowledge points and should *certainly not* be used as a substitute for the actual learning material. Please notice that I make *no promise* about the accuracy of statements appearing in these notes.

The course website could be found here:
<http://www.math.toronto.edu/nhoell/MAT224/>

Contents

1	Vector Spaces	3
1.1	(Real) Vector Space	3
1.2	Sub-spaces	4
1.3	Linear Combinations	5
1.4	Linear (In)dependence	7
1.5	Interlude on solving SLEs	9
1.6	Bases and Dimension	10
2	Linear Transformations	14
2.1	Linear Transformations	14

Chapter 1

Vector Spaces

1.1 (Real) Vector Space

1.1.1. **Definition of real vector space:** A real vector space is a set V together with scalar

- (a) **Closure under vector addition:** an operation called vector addition, which for each pair of vectors $\vec{x}, \vec{y} \in V$ produces another vector in V denoted $\vec{x} + \vec{y}$, (i.e. $\forall \vec{x}, \vec{y} \in V, \vec{x} + \vec{y} \in V$) and
- (b) **Closure under scalar multiplication:** an operation called multiplication by a scalar (a real number), which for each vector $\vec{x} \in V$, an each scalar $c \in \mathbb{R}$ produces another vector in V denoted $c\vec{x}$. (i.e. $\forall \vec{x} \in V, \forall c \in \mathbb{R}, c\vec{x} \in V$)

Furthermore, the two operations must satisfy the following axioms:(important)

- (a) $\forall \vec{x}, \vec{y}, \vec{z} \in V, (\vec{x} + \vec{y}) + \vec{z} = \vec{x} + (\vec{y} + \vec{z})$
- (b) $\forall \vec{v}, \vec{y} \in V, \vec{x} + \vec{y} = \vec{y} + \vec{x}$
- (c) $\exists \vec{0} \in V$ s.t. $\forall \vec{x} \in V, \vec{x} + \vec{0} = \vec{x}$ (Note that this property is a.k.a existence of additive identity)
- (d) $\forall \vec{x} \in V, \exists (-\vec{x}) \in V$ s.t. $\vec{x} + (-\vec{x}) = \vec{0}$ (Note that this property is a.k.a existence of additive inverse)
- (e) $\forall \vec{x}, \vec{y} \in V, c \in \mathbb{R}, c(\vec{x} + \vec{y}) = c\vec{x} + c\vec{y}$
- (f) $\forall \vec{x} \in V, c, d \in \mathbb{R}, (c + d)\vec{x} = c\vec{x} + d\vec{x}$

$$(g) \quad \forall \vec{x} \in V, c, d \in \mathbb{R}, (cd)\vec{x} = c(d\vec{x})$$

$$(h) \quad \forall \vec{x} \in V, 1\vec{x} = \vec{x}$$

1.1.6. **Propositions for a R-v.s.** Let V be a vector space. Then

(a) The zero vector is unique. Note that it might not necessarily be actually the zero vector in \mathbb{R}^n that we are somewhat used to use.

$$(b) \quad \forall \vec{x} \in V, 0\vec{x} = 0$$

(c) $\forall \vec{x} \in V$, the additive inverse is unique. Note that it might not necessarily be actually just (-1) times the vector in \mathbb{R}^n that we are somewhat used to use.

$$(d) \quad \forall \vec{x} \in V, \forall c \in \mathbb{R}, (-c)\vec{x} = -(c\vec{x})$$

1.2 Sub-spaces

1.2.4. **Usual definition of subspace applied to functions in $C^0(\mathbb{R})$.** Note that by $C^n(\cdot)$ we mean the function in this set are all of *Class* $-n$. Let $f, g \in C^0(\mathbb{R})$, let $c \in \mathbb{R}$. Then,

$$(a) \quad f + g \in C^0(\mathbb{R}), \text{ and}$$

$$(b) \quad cf \in C(\mathbb{R})$$

The proof of this lemma relies on limit theorems of calculus.

1.2.6. **(Intuitive) definition of (vector) subspace** Let V be a vector space and let $W \subseteq V$ be a subset. Then W is a (vector) subspace if W is a vector subspace itself under the operations of vector sum and scalar multiplication from V .

1.2.8. **Quick check rule for a subspace.** Let V be a vector subspace, and let W be a **non empty** subset of V . Then W is a subspace of V if and only if $\forall \vec{x}, \vec{y} \in W, \forall c \in \mathbb{R}$, we have $c\vec{x} + \vec{y} \in W$.

1.2.9. **Remark on the necessary condition of non-emptiness of subspace.** According to the definition of vector space that we gave in 1.1.1, a vector space must contain an additive identity element, hence it is necessary that we ensure $W \subseteq V$ (from 1.2.6) is not an empty set.

- 1.2.13. **Theorem: Intersection of sub-spaces is a subspace.** Let V be a vector space. Then the intersection of any collection of sub-spaces of V is a subspace of V .
- 1.2.14. **Corollary: Hyper planes in \mathbb{R}^n are sub-spaces of \mathbb{R}^n .** Let a_{ij} ($1 \leq i \leq m$), let $W_i = \{(x_1, \dots, x_n) \in \mathbb{R}^n | a_{i1}x_1 + \dots + a_{in}x_n = 0, \forall 1 \leq i \leq m\}$. Then W is a subspace of \mathbb{R}^n .

1.3 Linear Combinations

- 1.3.1. **Definitions regarding L.C. and derived spans.** Let S be a subset of a vector space V , that is $S \subseteq V$.
- (a) a *linear combination* of vectors in S is any sum $a_1\vec{x}_1 + \dots + a_n\vec{x}_n$, where the $a_i \in \mathbb{R}$, and the $x_i \in S$.
 - (b) we define the *Span* of a set of vectors as follows to consider the special case of $S \stackrel{?}{=} \emptyset \in V$.
Case1: $S \neq \emptyset$: In this case, we define $Span(S)$ to be all possible linear combinations using vectors in S .
Case2: $S = \emptyset$: In this case, we define $Span(S = \emptyset) = \{\vec{0}\}$. We call this the zero-space.
 - (c) If $W = Span(S)$, we say S *spans (or generates)* W .
- 1.3.4. **Span of a subset of a vector space is a subspace.** Let V be a vector space and let S be any subset of V . Then $Span(S)$ is a subspace of V .
- 1.3.5. **Sum of sets (with application to sub-spaces).** Let $W_1 \wedge W_2$ be sub-spaces of a vector space V . The sum of W_1 and W_2 is the set

$$W_1 + W_2 := \{\vec{x} \in V | \vec{x} = \vec{x}_1 + \vec{x}_2, \text{ for some } \vec{x}_1 \in W_1, \vec{x}_2 \in W_2\}$$

We think of the sum of the two sub-spaces (the two sets) as the set of vectors that can be built up from the vectors in W_1 and W_2 by linear combinations. Conversely, the vectors in the set $W_1 + W_2$ are precisely the vectors that can be broken down into the sum of a vector in W_1 and a vector in W_2 . One may find it helpful to view this as an analogue to a Cartesian product of the two set with a new constraint on the result.

1.3.6. **Example.** If $W_1 = \{(a_1, a_2) \in \mathbb{R}^2 | a_2 = 0\}$ and $W_2 = \{(a_1, a_2) \in \mathbb{R}^2 | a_1 = 0\}$, then $W_1 + W_2 = \mathbb{R}^2$, since every vector in \mathbb{R}^2 can be written as the sum of vector in W_1 and a vector in W_2 . For instance, we have $(5, -6) = (5, 0) + (0, -6)$, and $(5, 0) \in W_1$ and $(0, -6) \in W_2$.

1.3.8. **Proposition: The sum of spans of sets is the span of the union of the sets.** Let $W_1 = \text{Span}(S_1)$ and $W_2 = \text{Span}(S_2)$ be sub-spaces of a (the same) vector space V . Then $W_1 + W_2 = \text{Span}(S_1 \cup S_2)$. Notice that the proof of this gave the important idea of mutual inclusion in proving sets are equal to each other.

1.3.9. **The sum of sub-spaces is also a subspace.** Let W_1 and W_2 be sub-spaces of a vector space V . Then $W_1 + W_2$ is also a subspace of V .

Proof:

It is clear that $W_1 + W_2$ is non-empty, since neither W_1 nor W_2 is empty. Let \vec{x}, \vec{y} be two vectors in $W_1 + W_2$, let $c \in \mathbb{R}$. By our choice of \vec{x} and \vec{y} , we have

$$\begin{aligned} c\vec{x} + \vec{y} &= c(\vec{x}_1 + \vec{x}_2) + (\vec{y}_1 + \vec{y}_2) \\ &= (c\vec{x}_1 + \vec{y}_1) + (c\vec{x}_2 + \vec{y}_2) \in W_1 + W_2 \end{aligned}$$

Since W_1 and W_2 are sub-spaces of V , we have $(c\vec{x}_1 + \vec{y}_1) \in W_1$ and $(c\vec{x}_2 + \vec{y}_2) \in W_2$. Then by (1.2.8), we see that indeed $W_1 + W_2$ is a subspace of V . *Q.E.D.*

1.3.10. **Remark.** In general, if W_1 and W_2 are sub-spaces of V , then $W_1 \cup W_2$ will not be a subspace of V . For example, consider the two sub-spaces of \mathbb{R}^2 given in example (1.3.6). In that case $W_1 \cup W_2$ is the union of two lines through the origin in \mathbb{R}^2 .

1.3.11. **Proposition.** Let W_1 and W_2 be sub-spaces of vector space V and let W be a subspace of V such that $W \supseteq W_1 \cup W_2$, then $W \supseteq W_1 + W_2$. Informally speaking, this proposition saying: " $W_1 + W_2$ is the smallest subspace containing $W_1 \cup W_2$ ", i.e., Any subspace that contains $W_1 \cup W_2$ must be a super set of $W_1 + W_2$.

Proof:

We want to show: $W \supseteq W_1 \cup W_2 \implies W \supseteq W_1 + W_2$

Assume that $W \supseteq W_1 \cup W_2$. Let $w_1 \in W_1$, $w_2 \in W_2$.

We notice that $w_1, w_2 \in W_1 \cup W_2 \subseteq W$

$$\implies w_1, w_2 \in W$$

(Since W is a subspace, so it is closed under addition)

$$\implies w_1 + w_2 \in W$$

$$\implies W_1 + W_2 \subseteq W \iff W \supseteq W_1 + W_2$$

Q.E.D.

1.4 Linear (In)dependence

1.4.2. **Algebraic definition of linear dependence.** Let V be a vector space, and let $S \subseteq V$.

- (a) A *linear dependence* among the vectors of S is an equation $a_1\vec{x} + \dots + a_n\vec{x}_n = \vec{0}$ where the $x_i \in S$, and the $a_i \in \mathbb{R}$ are not all zero (i.e., at least one of the $a_i \neq 0$). In familiar¹ words, there exists a non-trivial solution to the equation mentioned above.
- (b) the set S is said to be *linearly dependent* if there exists a linear dependence among the vectors in S .

Remark: It can be shown that the geometric² definition and this are, in-fact, equivalent to each other. I will now produce the proof.

Proof of equivalence of definitions:

Let V be a vector space, and let $S \subseteq V$. Consider the following equa-

¹Familiar from MAT223, Prof. Jason Siefken's IBL(Inquiry Based Learning) notes.

²A set of vectors is said to be dependent if each other there exists a vector in this set, that it is in the Span of all other vectors in the set. I.e., There is some vectors in this set that are "redundant", it's position can be taken by some linear combination of the other vectors in the set.

tion:

$$\begin{aligned}
 & a_1\vec{x}_1 + a_2\vec{x}_2 + \dots + a_n\vec{x}_n = \vec{0}, \text{ where } \exists a_i \neq 0 \\
 & \text{(WLOG, assume that } a_n \neq 0\text{)} \\
 \implies & \frac{a_1\vec{x}_1 + a_2\vec{x}_2 + \dots + a_n\vec{x}_n}{a_n} = \vec{0} \\
 \implies & \vec{x}_n = - \sum_{i=1}^{n-1} a_i\vec{x}_i
 \end{aligned}$$

Notice that the result \vec{x}_n is in terms of all the other $(n-1)$ vectors in the set, hence a linear combination of those vectors, and this completes the proof. *Q.E.D.*

Re-Remark: We can also use this proof as an argument towards the following problem: Show that at least one of the vectors in a linearly dependent set is redundant. We could take a similar proof and argue that the linear combination could be written without at least one of the vectors.

1.4.4. Algebraic definition of linear independence. Let V be a vector space, and $S \subseteq V$. Then S is *linearly independent* if whenever we have $a_i \in \mathbb{R}$ and $x_i \in S$ such that $a_1\vec{x}_1 + \dots + a_n\vec{x}_n = \vec{0}$, then $a_i = 0, \forall i$. A more conceivable way to understand this is if the aforementioned equation exists and only exists a set of trivial solution then the vectors involved in the equation are *linearly independent*.

Remark: A set of vector is linearly independent *if and only if* it is not linearly dependent.

1.4.7. Propositions regarding linear (in)dependency.

- (a) Let S be a linearly dependent subset of a vector space V , and let S' be another subset of V that contains S . Then S' is also linearly dependent.
- (b) Let S be a linearly independent subset of vector space V and let S' be another subset of V that is contained in S . Then S' is also linearly independent.

Proof of (a): Since S is linearly dependent, there exists a linear dependence among the vectors in S , say, $a_1\vec{x}_1 + \dots + a_n\vec{x}_n = \vec{0}$. Since S is

contained in S' , this is also a linear dependence among the vectors in S' . Hence S' is linear dependent. *Q.E.D.*

Proof of (b): Consider any equation $a_1\vec{x}_1 + \dots + a_n\vec{x}_n = \vec{0}$, where the $a_i \in \mathbb{R}$, $\vec{x}_i \in S'$. Since S' is contained in S , we can also view this as a potential linear dependence among vectors in S . However, S is linearly independent, so it follows that all the $a_i = 0 \in \mathbb{R}$. Hence S' is also linearly independent. *Q.E.D.*

1.5 Interlude on solving SLEs

1.5.*. **Note Aside:** This section of the book is covered, although not rigorously but completely, in MAT223. Hence the vast majority of definitions and corollary in this section were omitted. Consult the book for more detail on this.

1.5.1. **Definition of (homogeneous) SLEs³** A system of m equations in n unknowns x_1, \dots, x_n of the form:

$$\begin{aligned} a_{11}\vec{x}_1 + \dots + a_{1n}\vec{x}_n &= b_1 \\ a_{21}\vec{x}_1 + \dots + a_{2n}\vec{x}_n &= b_2 \\ &\dots \\ a_{m1}\vec{x}_1 + \dots + a_{mn}\vec{x}_n &= b_m \end{aligned}$$

where the a_{ij} , $b_i \in \mathbb{R}$, is called a *system of linear equations*. The scalars a_{ij} are called coefficients or *weights* of the equations. We call this system **homogeneous** if and only if all the b_i are 0's.

1.5.2. **Definition of equivalent SLEs** Two systems of linear equations are said to be equivalent if their sets of solutions are the same (i.e., mutual inclusion of the two solution sets)

1.5.3. **Propositions on operations on SLEs⁴**

- (a) The system obtained by adding any multiple of any one equation to any second equation, while leaving the other other equations unchanged, is an equivalent system.

³System of Linear Equations

⁴This should be familiar from MAT223, operations involved in row reducing an augmented matrix for a system of linear equations

- (b) The system obtained by multiplying any one equation by a non-zero scalar and leaving the other equations unchanged is an equivalent system.
- (c) The system obtained by interchanging any two equations is an equivalent system.

1.5.13. **Corollary** If $m < n$, every homogeneous system of m linear equations in n unknowns has a non-trivial solution.

1.6 Bases and Dimension

1.6.1. **Definition of basis.** A subset S of a vector space V is called a basis if $V = \text{Span}(S)$ and the set S is linearly independent.

1.6.3. **Theorem.** Let V be a vector space, and let S be a non-empty subset of V . Then S is a basis of V if and only if $\forall \vec{x} \in V, \vec{x}$ can be written *uniquely* as a linear combination of the vectors in S .

1.6.6. **Theorem.** Let V be a vector space that has a finite spanning set, and let S be a linearly independent subset of V . Then there exists a basis S' of V , such that $S \subseteq S'$. Note that this theorem can be summarized as follows: Every linearly independent set of vectors could be extended to a basis. We do so by adding yet another vector that is linearly independent to all the vectors already in the set, but notice that this process should possibly be repeated but *not* infinite.

1.6.8. **Lemma on linear independence towards a set and a vector.** Let S be a linearly independent subset of V and let $\vec{x} \in V$, but $\vec{x} \notin S$. Then $S \cup \{\vec{x}\}$ is linearly independent if and only if $\vec{x} \notin \text{Span}(S)$.

1.6.10. **Theorem on cardinality of linearly independent set.** Let V be a vector space and let S be a spanning set for V , which has m elements. Then no linearly independent set in V can have more than m elements.

Proof:

To show that there are no linearly independent set in V that can have more than m elements in it, it suffices to show that every set in V that has more than m elements in it is linearly dependent. Let $S =$

$\{y_1, \dots, y_m\}$ and $S' = \{y_1, \dots, y_n\} \subset V$ where $n > m$. Now we consider the following equation:

$$a_1 \vec{x}_1 + \dots + a_n \vec{x}_n = \vec{0} \quad \text{where } \vec{x}_i \in S', a_i \in \mathbb{R} \quad (1.1)$$

Since S is a spanning set for V , then $\exists b_{ij} \in \mathbb{R}$, s.t. $\forall 1 \leq i \leq m$:

$$\vec{x}_i = b_{i1} \vec{y}_1 + \dots + b_{im} \vec{y}_m = \sum_{j=1}^m b_{ij} \vec{y}_j$$

Then we substitute the \vec{x}_i 's into equation (1.1):

$$a_1 \left(\sum_{j=1}^m b_{1j} \vec{y}_j \right) + \dots + a_n \left(\sum_{j=1}^m b_{nj} \vec{y}_j \right) = \vec{0} \quad (1.2)$$

Rearranging (1.2), we have:

$$\left(\sum_{j=1}^n b_{1j} a_j \right) \vec{y}_1 + \dots + \left(\sum_{j=1}^n b_{mj} a_j \right) \vec{y}_m = \vec{0} \quad (1.3)$$

Now we consider the following SLE(The coefficients of (1.3)):

$$\begin{cases} b_{11}a_1 + \dots + b_{1n}a_n & = 0 \\ b_{21}a_1 + \dots + b_{2n}a_n & = 0 \\ & \vdots \\ b_{m1}a_1 + \dots + b_{mn}a_n & = 0 \end{cases}$$

If we can find a set of a_1, \dots, a_n that are not all zero that solves the above SLE, then those scalars will give us a linear dependence among the vectors in S' in (1.1). But the above SLE is a system of homogeneous linear equations in the n unknowns a_i 's, hence since $m < n$, by Corollary (1.5.13), there exists a non-trivial solution. Then s' is linearly dependent and this completes the proof. $\mathcal{Q.E.D.}$

1.6.11. Bases of a vector space should have same cardinality. Let V be a vector space and let S and S' be two bases of V with m and m' elements, respectively. Then $m = m'$.

Proof: (Euclid's style)

Let S and S' with properties given as above. Since they are bases, we know: (By Theorem 1.6.10)

- (a) S is a spanning set and S' is a linearly independent set
 $\implies m' = |S'| \leq |S| = m$
- (b) S' is a spanning set and S is a linearly independent set
 $\implies m = |S| \leq |S'| = m'$

Then, $m' = m$.

Q.E.D.

1.6.12. Definitions of (in)finite-dimension

- (a) If V is a vector space with some finite basis (possibly empty), we say V is *finite-dimensional*. We say the vector space is *infinite-dimensional* otherwise.
- (b) Let V be a *finite-dimensional* vector space. The dimension of V , denoted as $\dim(V)$, is the number of elements in a (hence any) basis of V .
- (c) If $V = \{\vec{0}\}$, we define $\dim(V) = 0$. **Remark:** Please note that this is consistent with our definition of span of an empty set. We defined the span of an empty set to be $\{\vec{0}\}$, and hence $\{\vec{0}\}$ is the resulting space of all the possible linear combinations of vectors in the empty set (where there are none). Then the cardinality of the empty set (which is zero) is here defined as the dimension of the zero vector space.

1.6.13. Examples on dimensions of vector spaces. If we have a basis of V , then computing $\dim(V)$ is simply a matter of counting the number of vectors in a (hence any) basis for the vector space. We explore this by looking at the following examples

- (a) For each n , $\dim(\mathbb{R}^n) = n$. This is a consequence of the standard basis for \mathbb{R}^n is of the form: $\{\vec{e}_1, \dots, \vec{e}_n\}$ has n elements in it.
- (b) $\dim(P_n(\mathbb{R})) = n + 1$, since $|\{1, x^1, x^2, \dots, x^n\}| = n + 1$.⁵
- (c) The vector spaces $P(\mathbb{R})$ ⁶, $C^n(\mathbb{R})$, where $n \in \mathbb{N}^{\geq 0}$, are not of finite dimension, and hence are called *infinite dimensional*.

1.6.14. Corollary. Let W be a subspace of a finite-dimensional vector space V . Then $\dim(W) \leq \dim(V)$. Furthermore, $\dim(W) = \dim(V)$ if and only if $W = V$.

⁵The absolute value marks around a set return the cardinality of the set.

⁶Here $P(\mathbb{R})$ means the vector space of all polynomials that are $\mathbb{R} \rightarrow \mathbb{R}$.

1.6.15. **Corollary.** Let W be a subspace of \mathbb{R}^n defined by a system of homogeneous linear equations. The $\dim(W)$ is equal to the number of free variables in the corresponding echelon form of the equations.

1.6.18. **Inclusion-Exclusion principle of dimensions.** Let W_1 and W_2 be finite dimensional sub-spaces of a vector space V . Then,

$$\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2)$$

Chapter 2

Linear Transformations

2.1 Linear Transformations

2.1.1. **Definition of linear transformation.**¹ A function $T : V \rightarrow W$ is called a *linear mapping* or a *linear transformation* if it satisfies:

- (a) $\forall \vec{u}, \vec{v} \in V, T(\vec{u} + \vec{v}) = T(\vec{u}) + T(\vec{v})$
- (b) $\forall \alpha \in \mathbb{R}, \vec{v} \in V, T(\alpha \vec{v}) = \alpha T(\vec{v})$

2.1.2. **Proposition: alternative definition of L.T.s** A function $T : V \rightarrow W$ is a linear transformation if and only if $\forall \alpha, \beta \in \mathbb{R}, \forall \vec{u}, \vec{v} \in V, T(\alpha \vec{u} + \beta \vec{v}) = \alpha T(\vec{u}) + \beta T(\vec{v})$.

Proof(\implies):

Assuming that T is a linear transformation, then the definition in (2.1.1) must satisfy. Let $\alpha, \beta \in \mathbb{R}, \vec{u}, \vec{v} \in V$, then:

$$\begin{aligned} T(\alpha \vec{u} + \beta \vec{v}) &= T(\alpha \vec{u}) + T(\beta \vec{v}) && // \text{ by (a)} \\ &= \alpha T(\vec{u}) + \beta T(\vec{v}) && // \text{ by (b)} \end{aligned}$$

Proof(\impliedby):

Assuming the alternative definition, we want to show the definition given in (2.1.1). Since the quantifier is \forall , we can take $\alpha = \beta = 1$, (arbitrary) $\vec{u}, \vec{v} \in V$ in the alternative definition which directly yields

¹Familiar from MAT223

us (a) of (2.1.1). Then we take $\alpha \in \mathbb{R}, \beta = 0, \vec{u}, \vec{v} \in V$. In this case,

$$\begin{aligned} T(\alpha\vec{u} + \beta\vec{v}) &= T(\alpha\vec{u} + 0\vec{v}) \\ &= \alpha T(\vec{u}) + 0T(\vec{v}) \\ &= \alpha T(\vec{u}) \end{aligned}$$

Since $\alpha \in \mathbb{R}, \vec{u} \in V$ are arbitrary, this completes the proof. $\mathcal{Q.E.D.}$