

Honours Algebra

Quick Notes

Ian S.W. Ma

1 Vector Spaces

1.1 Solution of Simultaneous Linear Equations

Assume $F = \mathbb{Q}, \mathbb{R}$ or \mathbb{C} , where $a_{ij}, b_i \in F$, then

$$\sum_{j=1}^m a_{ij}x_j = b_i \quad \forall i \in [1, n] : i \in \mathbb{Z}$$

is a **system of linear Equations**

- if all b 's are 0 then the system is **homogenous**
- $L = \{x_1, \dots, x_m\}$ is the **solution set** of Equations

1.2 Fields and Vector Spaces

DEFINITION 1.2.1.

1. A **field** F is a set with functions:

- **addition** $= + : F \times F \rightarrow F; (\lambda, \mu) \mapsto \lambda + \mu$
- **multiplication** $= \cdot : F \times F \rightarrow F; (\lambda, \mu) \mapsto \lambda\mu$

such that $(F, +)$ and $(F \setminus \{0\}, \cdot)$ are abelian groups, with:

$$\lambda(\mu + \nu) = \lambda\mu + \lambda\nu \in F \quad \forall \lambda, \mu, \nu \in F$$

The neutral elements are called $0_F, 1_F$, in particular for all $\lambda, \mu \in F$

- $\lambda + \mu = \mu + \lambda \in F$
- $\lambda \cdot \mu = \mu \cdot \lambda \in F$
- $\lambda + 0_F = \lambda \in F$
- $\lambda \cdot 1_F = \lambda \in F$

For all $\lambda \in F$ there exists $-\lambda \in F$ such that $\lambda + (-\lambda) = 0_F \in F$

For all $\lambda \neq 0 \in F$ there exists $\lambda^{-1} \neq 0 \in F$ such that $\lambda(\lambda^{-1}) = 1_F \in F$

2. A **vector space** V over a field F is a pair consisting of an abelian group $V = (V, +)$ and a mapping

$$F \times V \rightarrow V; (\lambda, \vec{v})$$

such that for all $\lambda, \mu \in F$ and $\vec{v}, \vec{w} \in V$ the following identities hold:

- $\lambda(\vec{v} + \vec{w}) = \lambda\vec{v} + \lambda\vec{w}$ **Distributive Law**
- $(\lambda + \mu)\vec{v} = \lambda\vec{v} + \mu\vec{v}$ **Distributive Law**
- $\lambda(\mu\vec{v}) = (\lambda\mu)\vec{v}$ **Associativity Law**
- $1_F\vec{v} = \vec{v}$

LEMMA 1.2.1. If V is a vector space and $\vec{v} \in V$ then $0\vec{v} = \vec{0}$

LEMMA 1.2.2. If V is a vector space and $\vec{v} \in V$ then $(-1)\vec{v} = -\vec{v}$

LEMMA 1.2.3. If V is a vector space over a field F then $\lambda\vec{0} = \vec{0} \quad \forall \lambda \in F$

1.3 Product of Sets and of Vector Spaces

- **Cartesian product** of sets: $X_1 \times \dots \times X_n := \{(x_1, \dots, x_n) : x_i \in X_i \text{ for } 1 \leq i \leq n\}$, an element of this product is known as a product n-tuples.

There are special mappings called **projections** for a cartesian product

$$\begin{aligned} \text{pr}_i : X_1 \times \dots \times X_n &\rightarrow X_i \\ (x_1, \dots, x_n) &\mapsto x_i \end{aligned}$$

The cartesian product of n copies of a set X is written in short as X^n

$$\forall n, m \geq 0, X^n \times X^m \xrightarrow{\sim} X^{n+m}; ((x_1, \dots, x_n), (x_{n+1}, \dots, x_{n+m})) \mapsto (x_1, \dots, x_n, x_{n+1}, \dots, x_{n+m})$$

1.4 Vector Subspaces

DEFINITION 1.4.1. A subset U of a vector space V is called a **vector subspace** or **subspace** if U contains the zero vector ($\vec{0}$) and whenever \vec{u}, \vec{v} and $\lambda \in F$ we have $\vec{u} + \vec{v} \in U$ and $\lambda\vec{u} \in U$

PROPOSITION 1.4.1. Let T be a subset of vector space V over a field F . Then amongst all vector subspaces of V that include T there is a smallest vector subspace

$$\langle T \rangle = \langle T \rangle_F \subseteq V$$

DEFINITION 1.4.2. A subset S of a vector space V is called a **generating set** of a V if its span is all of the vector space. A vector space that has a finite generating set is **finitely generated**

DEFINITION 1.4.3. Check Definition 1.4.9 on Iain's (Not me I am Ian) note I dun think it's English

1.5 Linear Independence and Bases

DEFINITION 1.5.1. A subset $L = \{\vec{v}_1, \dots, \vec{v}_n\}$ of a vector subspace V is **linearly independent** if for all arbitrary scalars $\alpha_1, \dots, \alpha_n \in F$:

$$\sum_{i=1}^n \alpha_i \vec{v}_i = 0 \rightarrow \alpha_1 = \dots = \alpha_n = 0$$

DEFINITION 1.5.2. A subset $L = \{\vec{v}_1, \dots, \vec{v}_n\}$ of a vector subspace V is **linearly dependent** if it's not **linearly independent**, which means there exist some $\alpha_j \in \{a_1, \dots, a_n\}, \alpha_j \neq 0$ such that

$$\sum_{i=1}^n \alpha_i \vec{v}_i = 0$$

DEFINITION 1.5.3. A **basis of a vector space** B of a vector space V is a linearly independent generating set in V

DEFINITION 1.5.4. Let F be a field, V a vector space over F and $\vec{v}_1, \dots, \vec{v}_r \in V$ vectors. The *family* $(\vec{v}_i)_{1 \leq i \leq r}$ is a basis of V if and only if the following "evaluation"

$$\begin{aligned} \Phi : F^r &\rightarrow V \\ (\alpha_1, \dots, \alpha_r) &\mapsto \alpha_1 \vec{v}_1 + \dots + \alpha_r \vec{v}_r \end{aligned}$$

is a bijection

DEFINITION 1.5.5. The following for a subset E of a vector space V are equivalent: An isomorphism of a vector space to itself is called **an automorphism** of our vector space.

- Our subset E is a basis, ie. a linearly independent generating set;
- Our subset E is a minimal among all generating sets, meaning that $E \setminus \{\vec{v}\}$ does not generate V
- Our subset E is maximal among all linearly independent subsets, meaning that $E \cup \{\vec{v}\}$ is not linearly independent for any $\vec{v} \in V$

COROLLARY 1.5.1. Let V be a finitely generated vector space over a field F , then V is a basis

THEOREM 1.5.1. Let V be a vector space.

- If $L \subset V$ is a linearly independent subset and E is a minimal amongst all generating sets of our vector with $L \subseteq E$, then E is a basis.
- If $L \subseteq V$ is a generating set and if L is maximal amongst all linearly independent subsets of vector space with $L \subseteq E$, then L is a basis.

THEOREM 1.5.2. Let field F , F -vector space V and family of vectors $(\vec{v}_i)_{i \in I}$ from V , The following are equivalent:

- The family $(\vec{v}_i)_{i \in I}$ is a basis of V ;
- For each vector $\vec{v} \in V$ there is precisely one family $(a_i)_{i \in I}$ of elements of field F , almost all of which are zero and such that:

$$\vec{v} = \sum_{i \in I} a_i \vec{v}_i$$

1.6 Dimension of a vector space

THEOREM 1.6.1 (Fundamental Estimate of Linear Algebra). No linearly independent subset of a given vector space has more elements than a generating set. Thus if V is a vector space, $L \subset V$ a linearly independent subset and $E \subseteq V$ a generating set, then $|L| \leq |E|$

THEOREM 1.6.2 (Steinitz Exchange Theorem). Let V be a vector space, $L \subset V$ a finite linearly independent subset and $E \subseteq V$ a generating set. Then there is an injection $\phi : L \hookrightarrow E$ such that $(E \setminus \phi(L)) \cup L$ is also a generating set for V

LEMMA 1.6.1 (Exchange Lemma). Let V be a vector space, $M \subseteq V$ a linearly independent subset, and $E \subseteq V$ a generating subset, such that $M \subseteq E$. If $\vec{w} \in V \setminus M$ is a vector not belonging to M such that $M \cup \{\vec{w}\}$ is linearly independent, then there exists $\vec{e} \in E \setminus M$ such that $\{E \setminus \{\vec{e}\}\} \cup \{\vec{w}\}$ is a generating set for V

COROLLARY 1.6.1 (Cardinality of Bases). Let V be a finitely generated vector space.

- V has a finite basis
- V cannot have an infinite basis
- Any two bases of V have the same number of elements

DEFINITION 1.6.1. The cardinality of one (and by Cardinality of Bases each) basis of a finitely generated vector space V is called the **dimension** of V and will be denoted by $\dim(V)$. If the vector space is not finitely generated, then we write $\dim(V) = \infty$ and call V infinite dimensional. As usual, we will ignore the difference between infinities.

COROLLARY 1.6.2 (Cardinality Criterion for Bases). Let V be a finitely generated vector space.

- Each linearly independent subset $L \subset V$ has at most $\dim(V)$ elements, and if $|L| = \dim(V)$ then L is actually a basis
- Each generating set $E \subseteq V$ has at least $\dim(V)$ elements, and if $|E| = \dim(V)$ then E is actually a basis.

COROLLARY 1.6.3 (Dimension Estimate for Vector Subspaces). A proper vector subspace of a finite dimensional vector space has itself a strictly smaller dimension.

THEOREM 1.6.3 (The Dimension Theorem). Let V be vector space containing vector subspaces $U, W \subseteq V$. Then

$$\dim(U + W) + \dim(U \cap W) = \dim(U) + \dim(W)$$

1.7 Linear Mappings

DEFINITION 1.7.1. Let V, W be a vector spaces over a field F . A mapping $f : V \rightarrow W$ is called **linear** or more precisely **F-linearly** or even a **homomorphism of F -vector spaces** if for all $\vec{v}_1, \vec{v}_2 \in V$ and $\lambda \in F$ we have

$$\begin{aligned} f(\vec{v}_1 + \vec{v}_2) &= f(\vec{v}_1) + f(\vec{v}_2) \\ f(\lambda \vec{v}_1) &= \lambda f(\vec{v}_1) \end{aligned}$$

- A bijective linear mapping is called as **isomorphism** of vector spaces. If there is an isomorphism between two vector spaces we say them **isomorphic**.
- A **homomorphism** from one vector space to itself is called an **endomorphism** of our vector space.
- An isomorphism of a vector space to itself is called an **automorphism** of our vector space.

DEFINITION 1.7.2. A point that is sent to itself by a mapping is called a **fixed point** of the mapping. Given a mapping $f : X \rightarrow X$, we denote the set of fixed points by

$$X^f = \{x \in X : f(x) = x\}$$

DEFINITION 1.7.3. Two vector subspaces V_1, V_2 of a vector space V are called **complementary** if addition defines a bijection $V_1 \times V_2 \xrightarrow{\sim} V$

THEOREM 1.7.1 (The Classification of Vector Spaces by their Dimension). Let $n \in \mathbb{N}$. Then a vector space over a field F is isomorphic to F^n i.f.f it has dimension n

LEMMA 1.7.1 (Linear Mappings and Bases). Let V, W be vector spaces over F and let $B \subset V$ be a basis. Then restriction of a mapping gives a bijection

$$\begin{aligned} \text{Hom}_F(V, W) &\xrightarrow{\sim} \text{Maps}(B, W) \\ f &\mapsto f|_B \end{aligned}$$

PROPOSITION 1.7.1. • Every injective linear mapping $f : V \hookrightarrow W$ has a **left inverse**, in other words a linear mapping $g : W \rightarrow V$ such that $g \circ f = \text{id}_V$

- Every surjective linear mapping $f : V \twoheadrightarrow W$ has a **right inverse**, in other words a linear mapping $g : W \rightarrow V$ such that $g \circ f = \text{id}_W$

1.8 Rank-Nullity Theorem

DEFINITION 1.8.1. The **image** of a linear mapping $f : V \rightarrow W$ is the subset $\text{im}(f) = f(V) \subseteq W$. The **preimage** of the zero vector (**kernel**) of a linear mapping $f : V \rightarrow W$ is denoted by

$$\ker(f) := f^{-1}(0) = \{v \in V : f(v) = 0\}$$

The kernel is a vector subspace of V

LEMMA 1.8.1. A linear mapping $f : V \rightarrow W$ is injective if and only if its kernel is zero.

THEOREM 1.8.1 (Rank-Nullity Theorem). Let $f : V \rightarrow W$ be a linear mapping between vector spaces, then $\dim(V) = \dim(\ker f) + \dim(\text{im}(f))$

2 Linear Mappings and Matrices

2.1 Linear Mappings $F^m \rightarrow F^n$ and Matrices

THEOREM 2.1.1 (Linear mappings $F^m \rightarrow F^n$ and Matrices). Let F be a field and let $m, n \in \mathbb{N}$ be natural numbers. There is a bijection between the space of linear mappings $F^m \rightarrow F^n$ and the set of matrices with n rows and m columns and entries in F :

$$\begin{aligned} \mathbf{M} : \text{Hom}_F(F^m, F^n) &\xrightarrow{\sim} \text{Mat}(n \times m; F) \\ f &\mapsto [f] \end{aligned}$$

This attaches to each linear mapping f its **representing matrix** $\mathbf{M}(f) := [f]$. The columns of this matrix are the images under f of the standard basis elements of F^m :

$$[f] = (f(\vec{e}_1) | f(\vec{e}_2) | \dots | f(\vec{e}_m))$$

DEFINITION 2.1.1. Let $n, m, l \in \mathbb{N}$, F a field and let $A \in \text{Mat}(n \times m; F)$ and $B \in \text{Mat}(m \times l; F)$ be matrices. The **product** $A \circ B = AB \in \text{Mat}(n \times l; F)$ is the matrix defined by

$$(AB)_{ik} = \sum_{j=1}^m A_{ij} B_{jk}$$

THEOREM 2.1.2 (Composition of Linear Mapping and Products of Matrices). Let $g : F^l \rightarrow F^m$ and $f : F^m \rightarrow F^n$ be linear mappings. Then $[f \circ g] = [f] \circ [g]$

2.2 Basic Properties of Matrices

DEFINITION 2.2.1. A matrix A is called **invertible** if there exist matrices such that $BA = I$ and $AC = I$

will define an **elementary matrix** to be any square matrix that differs from the identity matrix in at most one entry.

DEFINITION 2.2.2.