Honours Algebra
Quick Notes

Ian S.W. Ma

1 Vector Spaces

1.1 Solution of Simultianeous 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**
- $L = \{x_1, ..., x_m\}$ 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** $= + : F \times F \to F; (\lambda, \mu) \mapsto \lambda + \mu$
   - **multiplication** $= \cdot : F \times F \to F; (\lambda, \mu) \mapsto \lambda\mu$

   such that $(F, +)$ ans $(F \backslash \{0\}, \cdot)$ 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 $\lambda \neq 0 \in F$ tehre 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 $V = (V, \dot{+})$ and a mapping
$$F \times V \to V; (\lambda, \overrightarrow{v})$$
such that for all $\lambda, \mu \in F$ and $\overrightarrow{v}, \overrightarrow{w} \in V$ the following identities hold:
   - $\lambda(\overrightarrow{v} + \overrightarrow{w}) = \lambda\overrightarrow{v} + \lambda\overrightarrow{w}$ **Distributive Law**
   - $(\lambda + \mu)\overrightarrow{v} = \lambda\overrightarrow{v} + \mu\overrightarrow{v}$ **Distributive Law**
   - $\lambda(\mu\overrightarrow{v}) = (\lambda\mu)\overrightarrow{v}$ **Associativity Law**
   - $1_F\overrightarrow{v} = \overrightarrow{v}$

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

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

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

1.3 Product of Sets and of Vector Spaces

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

There are special mappings called **projections** for a cartesian product
$$\text{pr}_i : X_i \times ... \times X_n \to X_i$$
$$(x_i, ..., x_n) \mapsto x_i$$
The cartesian product of n copies of a set X is written in short as X^n
$$\forall n, m \geq 0,\ X^n \times X^m \xrightarrow{\sim} X^{n+m}; ((x_1, ..., x_n), (x_{n+1}, ..., x_{n+m})) \mapsto (x_1, ..., x_n, x_{n+1}, x_{n+m})$$

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 ($\overrightarrow{0}$) and whenever $\overrightarrow{u}, \overrightarrow{v}$ and $\lambda \in F$ we have $\overrightarrow{u} + \overrightarrow{v} \in U$ and $\lambda\overrightarrow{u} \in U$

PROPOSITION 1.4.1. Let T be a subset od 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 $L = \{\overrightarrow{v_1}, ..., \overrightarrow{v_n}\}$ of a vector subspace V is **linearly independent** if for all arbitrary scalars $\alpha_1, ..., \alpha_n \in F$:

$$\sum_{i=1}^{n} \alpha_i \overrightarrow{v_i} = 0 \to \alpha_1 = ... = \alpha_n = 0$$

DEFINITION 1.5.2. A subset $L = \{\overrightarrow{v_1}, ..., \overrightarrow{v_n}\}$ of a vector subspace V is **linearly dependent** if it's not **linearly independent**, whcih mean there exist some $\alpha_j \in \{a_1, ..., a_n\}, \alpha_j \neq 0$ such that

$$\sum_{i=1}^{n} \alpha_i \overrightarrow{v_i} = 0$$

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 $\overrightarrow{v_1}, ..., \overrightarrow{v_r} \in V$ vectors. The *family* $(\overrightarrow{v_i})_{1 \leq i \leq r}$ is a basis of V if and only if the following "*evaluation*"

$$\Phi : F^r \to V$$
$$(\alpha_1, ..., \alpha_r) \mapsto \alpha_1 \overrightarrow{v}_1 + ... + \alpha_r \overrightarrow{v}_r$$

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 **anautomorphism** 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 $E \backslash \{\overrightarrow{v}\}$ does not generate V
- Our subset E is maximal among all linearly independent subsets, meaning that $E \cup \{\overrightarrow{v}\}$ is not linearly independent for any $\overrightarrow{v} \in V$

COROLLARY 1.5.1. Let V be a finitely generated vector space over a vield 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 isn a basis.
- If $L \subseteq V$ is a generating set and if L is maximal amongstall 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 $(\overrightarrow{v_i})_{i\in I}$ from V, The following are equivalent:

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

$$\overrightarrow{v} = \sum_{i\in I} a_i \overrightarrow{v_i}$$

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 then 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 $(E \backslash \phi(L)) \cup L$ 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, adn $E \subseteq V$ a generating subset, such that $M \subseteq E$. if $\overrightarrow{w} \in V \backslash M$ is a vector not belonging to M such that $M \cup \{\overrightarrow{w}\}$ is linearly independent, then there exists $\overrightarrow{e} \in E \backslash M$ such that $\{E \backslash \{\overrightarrow{e}\}\} \cup \{\overrightarrow{w}\}$ 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 $|E| = \dim(V)$ the 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 vectpr 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 $f : V \to W$ is called **linear** or more percisely **F-linearly** or even a **homomorphism of F-vector spaces** if for all $\overrightarrow{v}_1, \overrightarrow{v}_2 \in V$ and $\lambda \in F$ we have

$$f(\overrightarrow{v}_1 + \overrightarrow{v}_2) = f(\overrightarrow{v}_1) + f(\overrightarrow{v}_2)$$
$$f(\lambda\overrightarrow{v}_1) = \lambda f(\overrightarrow{v}_1)$$

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

DEFINITION 1.7.2. A point that is sent to itself br a mapping is called a **fixed point** of the mapping. Given a mapping $f : X \to X$, we donote 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** of 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

$$\mathrm{Hom}_F(V, W) \xrightarrow{\sim} \mathrm{Maps}(B, W)$$
$$f \mapsto f|_B$$

PROPOSITION 1.7.1.

- Every injective linar mapping $f : V \hookrightarrow W$ has a **left inverse**, in other words a linear mapping $g : W \to V$ such that $g \circ f = \mathrm{id}_V$
- Every surjective linear mapping $f : V \twoheadrightarrow W$ has a **right inverse**, in other words a linear mapping $g : W \to V$ such that $g \circ f = \mathrm{id}_W$

1.8 Rank-Nullity Throrem

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

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

The kernel is a vector subspace if V

LEMMA 1.8.1. A linear mapping $f : V \to W$ is injective if an only if it's kernel is zero.

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

2 Linear Mappings and Matrices

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

THEOREM 2.1.1 (Linear mappings $F^m \to F^n$ and Matrices)**.** Let F be a field and let $m, nin\mathbb{N}$ be neutral numbers. There is a nijection between the space of linear mappings $F^m \to F^n$ and the set of matrices woth n rows anf m columns and entries in F:

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

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

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

DEFINITION 2.1.1. Let $n, m, l \in \mathbb{N}$, F a field and let $A \in \mathrm{Mat}(n \times m; F)$ and $B \in \mathrm{Mat}(m \times l; F)$ be matrices. The **product** $A \circ B = AB \in \mathrm{Mat}(n \times l; F)$ 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 $g : F^l \to F^m$ and $f : F^m \to F^n belinearmappings.$ Then $[f \circ g] = [f] \circ [g]$

2.2 Basic Properties of Matrices

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

DEFINITION 2.2.2. will define an **elementary matrix** to be any square matrix that differs from the identity matrix in at most one entry.

THEOREM 2.2.1. Every square matrix with entries in a field can be written as a product if elementary matrices.

DEFINITION 2.2.3. Any matrix whose only non-zero entries lies on the diagonal, and which has first 1's along the diagonal and then 0's, is said to be in **Smith Normal Form**:

$$A_{ij} = \begin{cases} 0 \text{ if } i \neq j \\ 1 \text{ if } A_{(i+1)(j+1)} = 1 \\ 0 \text{ otherwise} \end{cases}$$

THEOREM 2.2.2 ((Transformation of a Matrix into Smith Normal Form)**.** For each matrix $A \in \mathrm{Mat}(n \times m; F)$ there exist invertable matrices P, Q such that PAQ is a matrix in Smith Normal Form.

DEFINITION 2.2.4. The **column rank** of a matrix $A \in \mathrm{Mat}(n \times m; F)$ is the dimension of the subsequence of F^n generated by the columns of A. Simmilarly, the **row rank** of A is the dimension of the subspace of F^m generated by the rows of A.

THEOREM 2.2.3. The column rank and the row rank of any matrix are equal.

Let's now refer the column and row rank as **rank** for the sake of not losing any generality.

DEFINITION 2.2.5. When the rank is as big as possible, meaning that it's equal to either the number of rows or number of columns (whichever is smaller), then the matrix has **full rank**

2.3 Abstract Linear Mappings and Matrices

THEOREM 2.3.1 (Abstract Linear Mappings and Matrices)**.** Let F be a field, V, W vector spaces over F with ordered bases $\mathcal{A} = (\overrightarrow{v}_1, ..., \overrightarrow{v}_m)$ and $\mathcal{B} = (\overrightarrow{w}_1, ..., \overrightarrow{w}_n)$. Then to each linear mapping $f : V \to W$ we assosiate bases a **representing matrix** ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ whose entried a_ij are defined by the identity

$$f(\overrightarrow{v}_j) = \sum_{i=1}^{n} a_{ij} \overrightarrow{w}_i \in W$$

This produces a bijection, which is event an isomorphismof vector spaces:

$$\mathbf{M}_{\mathcal{B}}^{\mathcal{A}} : \mathrm{Hom}_F(V, W) \xrightarrow{\sim} \mathrm{Mat}(n \times m; F)$$
$$f \mapsto_{\mathcal{B}} [f]_{\mathcal{A}}$$

We call $\mathbf{M}_{\mathcal{B}}^{\mathcal{A}}(f) =_{\mathcal{B}} [f]_{\mathcal{A}}$ the **epresenting matrix of the mappingfwith respect to the bases $\mathcal{A}$ and $\mathcal{B}$**

THEOREM 2.3.2 (The Representing Matrix of a Composition of Linear Mappings)**.** Let F be a field and U, V, W finite dimensional vector spaces over F with ordered bases $\mathcal{A}, \mathcal{B}, \mathcal{C}$. If $f : U \to V$ and $g : V \to W$ are linear mappings, then the representing matrixof the composition $g \circ f : U \to W$ is the matrix product of the representing matrix of f and g:

$${}_{\mathcal{C}}[g \circ f]_{\mathcal{A}} =_{\mathcal{C}} [g]_{\mathcal{B}} \circ_{\mathcal{B}} [f]_{\mathcal{A}}$$

DEFINITION 2.3.1. Let V be a finite dimensional vector space with an ordered basis $\mathcal{A} = (\overrightarrow{v}_1, ..., \overrightarrow{v}_m)$. We will denote the invese to the bijection of $\Phi_{\mathcal{A}} \xrightarrow{\sim} V, (\alpha_a, ..., \alpha_m)^T \mapsto \sum_{i=1}^{m} \alpha_i \overrightarrow{v}_i$ by

$$\overrightarrow{v} \mapsto_{\mathcal{A}} [\overrightarrow{v}]$$

THEOREM 2.3.3 (Representation of the Image of a Vector)**.** Let V, W be finite dimensional vector spaces over F with ordered bases $\mathcal{A}, \mathcal{B}$ and let $f : V \to W$ be a linear mapping. The following holds for $\overrightarrow{v} \in V$:

$${}_{\mathcal{B}}[f(\overrightarrow{v})] =_{\mathcal{B}} [f]_{\mathcal{A}} \circ_{\mathcal{A}} [\overrightarrow{v}]$$

2.4 Change of Matrix by Change of Basis

DEFINITION 2.4.1. Let $\mathcal{A} = (\overrightarrow{v}_1, ..., \overrightarrow{v}_n), \mathcal{B} = (\overrightarrow{w}_1, ..., \overrightarrow{w}_n)$ be ordered bses of the same F-vector space V. Then the matrix representing the identity mapping with respect to the bases ${}_{\mathcal{B}}[\mathrm{id}_V]_{\mathcal{A}}$ is called a **change of basis matrix**. By definition, its entries are given by the equalities $\overrightarrow{v}_j = \sum_{i=1}^{n} a_{ij}\overrightarrow{w}_i$

THEOREM 2.4.1 (Change of Basis)**.** Let V, W be finite dimensional vector spaces over F and let $f : V \to W$ br a linear mapping. Suppose that $\mathcal{A}, \mathcal{A}'$ are order bases of V and $\mathcal{B}, \mathcal{B}'$ are ordered bases of W. Then:

$$_{\mathcal{B}'}[f]_{\mathcal{A}'} =_{\mathcal{B}'} [\mathrm{id}_W]_{\mathcal{B}} \circ_{\mathcal{B}} [f]_{\mathcal{A}} \circ_{\mathcal{B}} [\mathrm{id}_V]_{\mathcal{A}'}$$

COROLLARY 2.4.1. Let V be a finite dimensional vector space and let $f : V \to V$ be an endomorphism of V. Suppose that $\mathcal{A}, \mathcal{A}'$ are ordered bases od V. Then

$$_{\mathcal{A}'}[f]_{\mathcal{A}'} =_{\mathcal{A}} [\mathrm{id}_V]^{-1}_{\mathcal{A}'} \circ_{\mathcal{A}} [f]_{\mathcal{A}} \circ_{\mathcal{A}} [\mathrm{id}_V]_{\mathcal{A}'}$$

THEOREM 2.4.2 (Smith Normal Form)**.** Let $f : V \to W$ be a linear mapping between finite dimensional F-vector spaces. There exist an order basis $\mathcal{A}$ of V and an ordered basis $\mathcal{B}$ of W, such that the representing matrix ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ has zero entries everywhere except possibly on one diagonal, and along the diagonaltherer are 1's first, followed by 0's

DEFINITION 2.4.2 (Trace)**.** The trace of a square matrix is defined to be the sum of its diagonal entries:

$$\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii}$$