

# Honours Algebra

## Quick Notes

Ian S.W. Ma

May 3, 2020

## 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 then  $\forall \vec{v} \in V, \quad 0\vec{v} = \vec{0}$

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

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

**EXAMPLE 1.3.1** (Examples of tuples).

- Vector space of  $n$ -tuples over  $F$ :  $V = F^n$
- Vector space as space around us

### 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**

$$S \subseteq V \wedge \text{span}(S) = V \Rightarrow S \text{ is a generating set of } V$$

**DEFINITION 1.4.3.** If  $X$  is a set, then the set of all subsets  $\mathcal{P}(X) = \{U : U \subseteq X\}$  of  $X$  is called **power set** of  $X$ . We call the subset of  $\mathcal{P}(X)$  a **system of subsets of  $X$** . Given such a system  $\mathcal{U} \subseteq \mathcal{P}(X)$  we can create two new subsets of  $X$ , the **union** and the **intersection** of the set of our system  $\mathcal{U}$  as follows:

$$\begin{aligned} \bigcup_{U \in \mathcal{U}} U &= \{x \in X : \text{there is } U \in \mathcal{U} \text{ with } x \in U\} \\ \bigcap_{U \in \mathcal{U}} U &= \{x \in X : x \in U \quad \forall U \in \mathcal{U}\} \end{aligned}$$

## 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 mean 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  $V$

$$\text{span}(B) = V \wedge B \text{ is linearly independent} \Rightarrow B \text{ is a basis of } V$$

**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 a **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** (The existence of a basis). 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.

**DEFINITION 1.5.6** (To infinity but not beyond). Let  $X$  be a set and  $F$  a field. The set  $\text{Maps}(X, F)$  of all mappings  $f : X \rightarrow F$  becomes an  $F$ -vector space with the operations of pointwise addition and multiplication by a scalar. The subset of all mappings with send almost all elements of  $X$  to 0 is a vector subspace

**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  $|E| = \dim(V)$  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** (Definition of homomorphism, isomorphism, and automorphism). 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  $V$  over a field  $F$  is isomorphic to  $F^n$  i.f.f.  $\dim(V) = n$

**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  $\exists$  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  $\exists$  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 **invertable** if there exist matrices such that  $BA = I$  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 of elementary matrices.

**DEFINITION 2.2.3.** Any matrix whose only non-zero entries lie 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  $A \in \text{Mat}(n \times m; F)$  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  $A \in \text{Mat}(n \times m; F)$  is the dimension of the subsequence of  $F^n$  generated by the columns of  $A$ . Similarly, 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 to 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**

$$\text{rank}(M) = \min(\{\text{rowrank}(M), \text{colrank}(M)\}) \Rightarrow M \text{ has full rank}$$

## 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  $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_m)$  and  $\mathcal{B} = (\vec{w}_1, \dots, \vec{w}_n)$ . Then to each linear mapping  $f : V \rightarrow W$  we associate a **representing matrix**  ${}_B[f]_A$  whose entries  $a_{ij}$  are defined by the identity

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

This produces a bijection, which is even an isomorphism of vector spaces:

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

We call  $\mathbf{M}_B^A(f) = {}_B[f]_A$  the **representing matrix of the mapping with 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  $f : U \rightarrow V$  and  $g : V \rightarrow W$  are linear mappings, then the representing matrix of the composition  $g \circ f : U \rightarrow W$  is the matrix product of the representing matrix of  $f$  and  $g$ :

$${}_C[g \circ f]_A = {}_C[g]_B \circ {}_B[f]_A$$

**DEFINITION 2.3.1.** Let  $V$  be a finite dimensional vector space with an ordered basis  $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_m)$ . We will denote the inverse to the bijection of  $\Phi_{\mathcal{A}} : V \xrightarrow{\sim} F^m, (\alpha_1, \dots, \alpha_m)^T \mapsto \sum_{i=1}^m \alpha_i \vec{v}_i$  by

$$\vec{v} \mapsto {}_{\mathcal{A}}[\vec{v}]$$

**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  $f : V \rightarrow W$  be a linear mapping. The following holds for  $\vec{v} \in V$ :

$${}_B[f(\vec{v})] = {}_B[f]_A \circ {}_{\mathcal{A}}[\vec{v}]$$

## 2.4 Change of Matrix by Change of Basis

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

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

$${}_{B'}[f]_{A'} = {}_{B'}[\text{id}_W]_{B'} \circ {}_B[f]_A \circ {}_B[\text{id}_V]_{A'}$$

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

$${}_{A'}[f]_{A'} = {}_{A'}[\text{id}_V]_{A'}^{-1} \circ {}_A[f]_A \circ {}_A[\text{id}_V]_{A'}$$

**THEOREM 2.4.2** (Smith Normal Form). Let  $f : V \rightarrow W$  be a linear mapping between finite dimensional  $F$ -vector spaces. There exist an ordered basis  $\mathcal{A}$  of  $V$  and an ordered basis  $\mathcal{B}$  of  $W$ , such that the representing matrix  ${}_B[f]_A$  has zero entries everywhere except possibly on one diagonal, and along the diagonal there 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:

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

- Let  $A \in \text{Mat}(n \times m, F)$ ,  $B \in \text{Mat}(m \times n, F)$ , then  $\text{tr}(AB) = \text{tr}(BA)$
- Let  $f : V \rightarrow W$  and  $g : W \rightarrow V$  two linear mappings where  $V$  and  $W$  are both finite dimensional  $F$ -vector spaces, then  $\text{tr}(fg) = \text{tr}(gf)$
- Let  $V$  be a finite dimensional  $F$ -vector space and let  $f : V \rightarrow V$  be an idempotent, that is  $f^2 = f$ , then  $\text{tr}(f) = \dim(\text{im } f)$
- Let  $V$  be a finite dimensional  $F$ -vector space and  $f : v \rightarrow V$  a linear mapping, then  $\text{tr}(((f \circ) | \text{End}_F(V)) = (\dim_F V) \text{tr}(f | V))$

## 3 Rings and Modules

### 3.1 Rings

**DEFINITION 3.1.1.** A **ring** is a set with two operations  $(R, +, \cdot)$  that satisfy:

1.  $(R, +)$  is an abelian group
2.  $(R, \cdot)$  is a **monoid**, meaning that the second operation  $\cdot : R \times R \rightarrow R$  is associative and that there is an **identity element**  $1 = 1_R \in R$ , often called just the **identity**, with the property that  $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$
3. The Distributive laws hold, meaning that for all  $a, b, c \in R$

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) && \text{addition} \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c) && \text{multiplication} \end{aligned}$$

A ring which element is commutative, that means  $a \cdot b = b \cdot a \quad \forall a, b \in R$ , is a **commutative ring**

**PROPOSITION 3.1.1** (Divisibility by Sum). A natural number is divisible by 3 (respectively by 9) precisely when the sum of its digits is divisible by 3 (or 9)

**DEFINITION 3.1.2.** A **field** is a non-zero commutative ring  $F$  in which every non-zero element  $a \in F$  has an inverse  $a^{-1} \in F$ , that is an element  $a^{-1}$  with the property that  $a \cdot a^{-1} = a^{-1} \cdot a = 1$

**PROPOSITION 3.1.2.** Let  $m$  be a positive integer. The commutative ring  $\mathbb{Z}/m\mathbb{Z}$  is a field i.f.f.  $m$  is prime.

## 3.2 Properties of Rings

**LEMMA 3.2.1** (Multiplying by zero and negatives). Let  $R$  be a ring and let  $a, b \in R$ . Then:

1.  $0a = 0 = a0$
2.  $(-a)b = -(ab) = a(-b)$
3.  $(-a)(-b) = ab$

**DEFINITION 3.2.1.** Let  $m \in \mathbb{Z}$ . The  **$m$ -th multiple**  $ma$  of an element  $a$  in an abelian group  $R$  is:  $ma = a + a + \dots + a$  if  $m > 0$  (sum of  $m$   $a$ 's). Otherwise  $0a = 0$  and  $(-m)a = -(ma)$

**LEMMA 3.2.2** (Rules of multiples). Let  $R$  be a ring, let  $a, b \in R$  and  $m, n \in \mathbb{Z}$ . Then:

1.  $m(a + b) = ma + mb$
2.  $(m + n)a = ma + na$
3.  $m(na) = (mn)a$
4.  $m(ab) = (ma)b = a(mb)$
5.  $(ma)(nb) = (mn)(ab)$

**DEFINITION 3.2.2.** Let  $R$  be a ring. An element  $a \in R$  is called a **unit** if it is **invertable** in  $R$  or in other words **has a multiplicative inverse in**  $R$ , meaning that  $\exists a^{-1} \in R$  such that

$$aa^{-1} = 1 = a^{-1}a$$

**PROPOSITION 3.2.1.** The set  $R^\times$  of units in a ring  $R$  forms a group under multiplication.

**DEFINITION 3.2.3** (Zero-divisor). In a ring  $R$  a non-zero element  $a$  is called a **zero-divisor** or **divisor of zero** if there exists a non-zero element  $b$  such that either  $ab = 0$  or  $ba = 0$

$$a \neq 0 \in R, \exists b \neq 0 \in R \text{ s.t. } ab = 0 \cup ba = 0 \Rightarrow a \text{ is a zero divisor}$$

**DEFINITION 3.2.4** (Integral domain). An **integral domain** is a non-zero commutative ring that has no zero-divisors, therefore if  $D$  is an integral domain then:

1.  $ab = 0 \Rightarrow a = 0$  or  $b = 0$ , and
2.  $a, b \neq 0 \Rightarrow ab \neq 0$

**PROPOSITION 3.2.2** (Cancellation Law for Integral Domains). Let  $R$  be an integral domain and let  $a, b, c \in R$ . If  $ab = ac \wedge a \neq 0 \Rightarrow b = c$

**PROPOSITION 3.2.3.** Let  $m$  be a natural number. The  $\mathbb{Z}/m\mathbb{Z}$  is an integral domain i.f.f.  $m$  is prime

**THEOREM 3.2.1.** Every finite integral domain is a field

### 3.3 Polynomials

**DEFINITION 3.3.1.** Let  $R$  be a ring. A **polynomial** over  $R$  is an expression of the form

$$P = a_0 + a_1X + a_2X^2 + \dots + a_mX^m$$

for some  $m \in \mathbb{N} \setminus \{0\}$  and elements  $a_i \in R$  for  $0 \leq i \leq m$ . The set of all Polynomials over  $R$  is denoted by  $R[X]$ . In case  $a_m$  is not zero, the polynomial  $P$  has a degree of  $m$ , written  $\deg(P) = m$ , where  $a_m$  is the leading coefficient. When the leading coefficient is 1 the polynomial is a **monic** polynomial, linear for  $a_1$ , quadratic for  $a_2$ , then cubic for  $a_3$ .

**DEFINITION 3.3.2.** With the definition in the set  $R[X]$  becomes a ring called the **ring of polynomials with coefficients in**  $R$ , or **over**  $R$ . The zero and the identity of  $R[X]$  are the zero and identity of  $R$  resp.

**LEMMA 3.3.1.**

1. If a ring  $R$  with no zero-divisors, then  $R[X]$  has no zero-divisors and  $\deg(PQ) = \deg(P) + \deg(Q)$  for all non-zero  $P, Q \in R[X]$
2. If  $R$  is an integral domain then so is  $R[X]$ , so if  $R^\times$  is an integral domain then so is  $R[X]^\times$

**THEOREM 3.3.1** (Division and Remainder). Let  $R$  be an integral domain and let  $P, Q \in R[X]$  with  $Q$  monic. Then  $\exists$  unique  $A, B \in R[X]$  such that  $P = AQ + B$  and  $\deg(B) < \deg(Q)$  or  $B = 0$

**DEFINITION 3.3.3.** Let  $R$  be a commutative ring and  $P \in R[X]$  a polynomial. Then the polynomial  $P$  can be evaluated at the element  $\lambda \in R$  to produce  $P(\lambda)$  by replacing the powers of  $X$  in the polynomial  $P$  by the corresponding powers of  $\lambda$  in the polynomial  $P$  by the corresponding powers of  $\lambda$ . In this way we have a mapping  $R[X] \rightarrow \text{Maps}(R, R)$

This is the percise mathematical descrption of thinking of a polynomial as a function. An element  $\lambda \in R$  is a root of  $P$  is  $P(\lambda) = 0$

**PROPOSITION 3.3.1.** Let  $R$  be a commutative ring, let  $\lambda \in R$  and  $P(X) \in R[X]$ . Then  $\lambda$  is a root of  $P(X)$  i.f.f.  $(X - \lambda)$  divides  $P(X)$

**THEOREM 3.3.2.** Let  $R$  be a field, or more generally an integral domain. Then a non-zero polynomial  $P \in R[X] \setminus \{0\}$  has at most  $\deg(P)$  roots in  $R$

**DEFINITION 3.3.4.** A field  $F$  is algebraically closed if each non-constant polynomial  $P \in F[X] \setminus F$  with coefficients in our field has a root in our field  $F$

**THEOREM 3.3.3** (Fundamental Theorem of Algebra). The field of complex numbers  $\mathbb{C}$ , is algebraically closed.

**THEOREM 3.3.4.** If  $F$  is an algebraically closed field, then every non-zero polynomial  $P \in F[X] \setminus \{0\}$  **decomposes into linear factors**

$$P = c \prod_{i=1}^n (X - \lambda_i)$$

with  $n \geq 0, c \in F^\times$  and  $\lambda_1, \dots, \lambda_n \in F$

### 3.4 Homomorpghism, Ideals and Subrings

**DEFINITION 3.4.1.** Let  $R, S$  be rings. A mapping  $f : R \rightarrow S$  is a **ring homomorphism** if the following hold for all  $x, y \in R$ :

$$\begin{aligned} f(x + y) &= f(x) + f(y) \\ f(xy) &= f(x)f(y) \end{aligned}$$

**LEMMA 3.4.1.** Let  $R, S$  be rings and  $f : R \rightarrow S$  a ring homomorphism. Then for all  $x, y \in R, m \in \mathbb{Z}$ :

1.  $f(0_r) = 0_s$  Where  $0_R, 0_S$  are the zeros of the resptive ring
2.  $f(-x) = -f(x)$
3.  $f(x - y) = f(x) - f(y)$
4.  $f(mx) = mf(x)$

**DEFINITION 3.4.2.** A subset  $I$  of a ring  $R$  is an **ideal**, written  $I \trianglelefteq R$ , if the following hold:

1.  $I \neq \emptyset$
2.  $I$  is closed under subtraction
3.  $\forall i \in I, r \in R : ir, ri \in I$

**DEFINITION 3.4.3.** Let  $R$  be a commutative ring and let  $T \subset R$ . Then the **ideal of  $R$  generated by  $T$**  is the set

$${}_R\langle T \rangle = \left\{ \sum_{i=1}^m r_i t_i : t_1, \dots, t_m \in T, r_1, \dots, r_m \in R \right\}$$

**EXAMPLE 3.4.1.**

- Let  $m \in \mathbb{Z}$ . Then  ${}_Z\langle m \rangle = m\mathbb{Z}$
- Let  $P \in \mathbb{R}[X]$ . Then  ${}_{\mathbb{R}[X]}\langle P \rangle = \{AP : A \in \mathbb{R}[X]\} = \{Q : P \text{ divides } Q \text{ in } \mathbb{R}[X]\}$

**PROPOSITION 3.4.1.** Let  $R$  be a commutative ring and let  $T \subseteq R$ . Then  ${}_R\langle T \rangle$  is the smallest ideal of  $R$  that contains  $T$

**DEFINITION 3.4.4.** Let  $R$  be a commutative ring. An ideal  $I$  of  $R$  is called a **principal ideal** if  $I = \langle t \rangle$  for some  $t \in R$

**DEFINITION 3.4.5.** Let  $R, S$  be rings with zero elements  $0_R, 0_S$  resp and let  $f : R \rightarrow S$  be a ring homomorphism. Since  $f$  is in particular a group homomorphism from  $(R, +)$  to  $(S, +)$ , ther kernel of  $f$  already has a meaning:  $\ker(f) = \{r \in R : f(r) = 0_S\}$ .

**PROPOSITION 3.4.2.** Let  $R$  and  $S$  be rings and  $f : R \rightarrow S$  a ring homomorphism. Then  $\ker(f)$  is an ideal of  $R$ .

**LEMMA 3.4.2.**  $f$  is injective i.f.f.  $\ker(f) = \{0\}$

**LEMMA 3.4.3.** The intersection of any collection of ideals of a ring  $R$  is an ideal of  $R$

**LEMMA 3.4.4.** Let  $I, J$  be ideals of ring  $R$ . Then  $I + J = \{a + b : a \in I, b \in J\}$  is an ideal of  $R$

**DEFINITION 3.4.6** (subring). Let  $R$  be a ring. A subset  $R'$  of  $R$  is a **subring** of  $R$  if  $R'$  itself is a ring under the operations of addition and multiplication defined in  $R$

**EXAMPLE 3.4.2.**  $\forall$  ring  $R$ ,  $\{0\}, R$  are always the subrings of  $R$

**PROPOSITION 3.4.3** (Test of a subring). Let  $R'$  be a subset of a ring  $R$ . Then  $R'$  is a subring i.f.f.

1.  $R'$  has a multiplicative identity, and
2.  $R'$  is closed under subtraction:  $a, b \in R' \rightarrow a - b \in R'$ , and
3.  $R'$  is closed under multiplication

**PROPOSITION 3.4.4.** Let  $R$  and  $S$  be subrings and  $f : R \rightarrow S$  a ring homomorphism

1. If  $R'$  is a subring of  $R$  then  $f(R')$  is a subring of  $S$ . In particular,  $\text{im}(f)$  is a subring of  $S$
2. Assume that  $f(1_R) = 1_S$ . Then if  $x$  is a unit in  $R$ ,  $f(x)$  is a unit in  $S$  and  $(f(x))^{-1} = f(x^{-1})$ . In this case  $f$  restricts to a group homomorphism  $f|_{R^\times} : R^\times \rightarrow S^\times$

### 3.5 Equivalece Relations

**DEFINITION 3.5.1.** A **relation**  $R$  on a set  $X$  is a subset  $R \subseteq X \times X$ . In this context, and only in this context, we write  $xRy$  instead of  $(x, y) \in R$ .  $R$  is an **equivalence relation** on  $X$  when for all  $x, y, z \in X$  the following holds:

1. **Reflexivity:**  $xRx$
2. **Symmetry:**  $xRy \Leftrightarrow yRx$
3. **Transitivity:**  $(xRy \cap yRx) \rightarrow xRz$

**DEFINITION 3.5.2.** Suppose that  $\sim$  is an equivalence relation on a set  $X$ . For  $x \in X$  the set  $E(x) := \{z \in X : z \sim x\}$  is called the **equivalence class** of  $x$ . A subset  $E \subseteq X$  is called an **equivalence class** for our equivalence relation if there is an  $x \in X$  for which  $E = E(x)$ . An element of an equivalence relation is called a **representative** of the class. A subset  $Z \subseteq X$  contains percisely one element from each equivalenceclass is called a **system of representatives** for the equivalence relation.

**DEFINITION 3.5.3.** Given an equivalence relation  $\sim$  on the set  $X$  we will denote the set of equivalence classes, which is a subset of the power set  $\mathcal{P}(X)$ , by

$$(X/\sim) := \{E(x) : x \in X\}$$

**EXAMPLE 3.5.1.** Let  $\equiv$  be the equivalence relation of " $a \equiv b \pmod{m}$ ". Then  $(\mathbb{Z}/\equiv) = \mathbb{Z}/m\mathbb{Z}$

**DEFINITION 3.5.4.**  $g : (X/\sim) \rightarrow Z$  is **well-defined** if  $\exists$  a mapping  $f : X \rightarrow Z$  such that  $f$  has the property  $x \sim y \rightarrow f(x) = f(y)$  and  $g = \bar{f}$

### 3.6 Factor Rings and the First Isomorphism Theorem

**DEFINITION 3.6.1** (Coset). Let  $R$  be a ring,  $I \trianglelefteq R$  be an ideal in ring  $R$ . The set

$$x + I = \{x + i : i \in I\} \subseteq R$$

is a **coset of  $I$  in  $R$**  or the **coset of  $x$  with respect to  $I$  in  $R$**

**DEFINITION 3.6.2.** Let  $R$  be a ring,  $I \trianglelefteq R$  an ideal, and  $\sim$  the equivalence relation defined by  $x \sim y \Leftrightarrow x - y \in I$ . Then  $R/I$ , **the factor ring of  $R$  by  $I$**  or the **quotient of  $R$  by  $I$** , is the set  $(R/\sim)$  of cosets of  $I$  in  $R$ .

**THEOREM 3.6.1.** Let  $R$  be a ring and  $I \trianglelefteq R$  and ideal. Then  $R/I$  is a ring, where the operation of addition is defined by

$$(x + I) + (y + I) = (x + y) + I \quad \forall x, y \in R$$

and multiplication is defined by

$$(x + I)(y + I) = xy + I \quad \forall x, y \in R$$

**THEOREM 3.6.2** (The Universal Property of Factor Rings). Let  $R$  be a ring and  $I$  an ideal of  $R$ :

- The mapping  $\text{can} : R \rightarrow R/I$  sending  $r$  to  $r + I$  for all  $r \in R$  is a surjective ring homomorphism with kernel  $I$
- If  $f : R \rightarrow S$  is a ring homomorphism with  $f(I) = \{0_S\}$ , so that  $I \subseteq \ker(f)$ , then there is a unique ring homomorphism  $\bar{f} : R/I \rightarrow S$  such that  $f = \bar{f} \circ \text{can}$

**THEOREM 3.6.3** (First Isomorphism Theorem for Rings). Let  $R$  and  $S$  be rings. Then every ring homomorphism  $f : R \rightarrow S$  induces a ring isomorphism

$$\bar{f} : R/\ker f \xrightarrow{\sim} \text{im } f$$

### 3.7 Modules and All That

**DEFINITION 3.7.1.** A (left) **module  $M$  over a ring  $R$**  is a pair consisting if an abelian group  $M = (M, +)$  and a mapping

$$\begin{aligned} R \times M &\rightarrow M \\ (r, a) &\mapsto ra \end{aligned}$$

such that for all  $r, s \in R$  and  $a, b \in M$  the following indentities hold:

$$\begin{aligned} r(a + b) &= ra + rb \\ (r + s)a &= ra + sa \\ r(sa) &= (rs)a \\ 1_R a &= a \end{aligned}$$

**LEMMA 3.7.1.** Let  $R$  be a ring and  $M$  an  $R$ -module:

1.  $0_R a = 0_M \quad \forall a \in M$
2.  $r 0_M = 0_M \quad \forall r \in R$
3.  $(-r)a = r(-a) = -(ra) \quad \forall r \in R, a \in M$

**DEFINITION 3.7.2.** Let  $R$  be a ring and let  $M, N$  be  $R$ -modules. A mapping  $f : M \rightarrow N$  is an  **$R$ -homomorphism** or **homomorphism** if the following hold for all  $a, b \in M$  and  $r \in R$

$$\begin{aligned} f(a + b) &= f(a) + f(b) \\ f(ra) &= rf(a) \end{aligned}$$

The kernel of  $f$  is  $\ker f = \{a \in M : f(a) = 0_N\} \subseteq M$  and the image of  $f$  is  $\text{im } f = \{f(a) : a \in M\} \subseteq N$ . If  $f$  is a bijection then it is an  **$R$ -module isomorphism** or **isomorphism** ( $M \simeq N$ )

**DEFINITION 3.7.3.** A non-empty subset  $M'$  of an  $R$ -module  $M$  is a submodule if  $M'$  is an  $R$ -module with respect to the operations of the  $R$ -module  $M$  restricted to  $M'$

**PROPOSITION 3.7.1** (Test for a submodule). Let  $R$  be a ring and  $M$  an  $R$ -module. A subset  $M'$  of  $M$  is a submodule i.f.f.

1.  $0_M \in M'$
2.  $a, b \in M' \Rightarrow a - b \in M'$
3.  $r \in R, ai \in M' \Rightarrow ra \in M'$

**LEMMA 3.7.2.** Let  $f : M \rightarrow N$  be an  $R$ -homomorphism. The  $\ker f$  is a submodule of  $M$  and  $\text{im } f$  is a submodule of  $N$ .

**LEMMA 3.7.3.** Let  $R$  be a ring,  $M, N$  be  $R$ -modules and let  $f : M \rightarrow N$  be an  $R$ -homomorphism. Then  $f$  is injective i.f.f.  $\ker f = \{0_M\}$

**DEFINITION 3.7.4.** Let  $R$  be a ring,  $M$  and  $R$ -module and let  $T \subseteq M$ . The the submodule of  $M$  generated by  $T$  is the set

$${}_R\langle T \rangle = \{r_1 t_1 + \dots + r_m t_m : t_1, \dots, t_m \in T, r_1, \dots, r_m \in R\}$$

together with the zero element in the case  $T = \emptyset$ . If  $T = t_1, \dots, t_n$  a finite set, we can write  ${}_R\langle T \rangle$  as  ${}_R\langle t_1, \dots, t_n \rangle$ . The module  $M$  is **finitely generated** if it is generated bt a finite set:  $M = {}_R\langle t_1, \dots, t_n \rangle$ . It is called **cyclic** if it is generated by a singleton:  $M = {}_R\langle t \rangle$

**EXAMPLE 3.7.1.**

- A cyclic group = a cyclic  $\mathbb{Z}$ -module
- Let  $R$  be a commutative ring. The the ideal generated by  $T \subseteq R$  = submodule of  $R$  generated by  $T$ .
- A principal ideal of  $R$  = cyclic submodule of  $R$
- $\{0_M\}$  is always a cyclic submodule of an  $R$ -module  $M$ , generated by the element  $0_M$ :  ${}_R\langle 0_M \rangle = \{0_M\}$

**LEMMA 3.7.4.** Let  $T \subseteq M$ . The  ${}_R\langle T \rangle$  is the smallest submodule of  $M$  that contains  $T$

**LEMMA 3.7.5.** The intersection of any collection of submodules of  $M$  is a submodule of  $M$ .

**LEMMA 3.7.6.** Let  $M_1, M_2$  be submodules of  $M$ , Then  $M_1 + M_2 = \{a + b : a \in M_1, b \in M_2\}$  is a submodule of  $M$

**DEFINITION 3.7.5.** Let  $R$  be a ring,  $M$  an  $R$ -module and  $N$  a submodule of  $M$ . For each  $a \in M$  the coset of  $a$  with respect to  $N$  in  $M$  is

$$a + N = \{a + b : b \in N\}$$

**THEOREM 3.7.1** (The Universal Property of Factor Modules). Let  $R$  be a ring, let  $L$  and  $M$  be  $R$ -modules, and  $N$  a submodule of  $M$ .

1. The mapping  $g : M \rightarrow M/N$  sending  $a$  to  $a + N$  for all  $a \in M$  is surjective  $R$ -homomorphism with kernel  $N$ :  $\ker g = N$
2. If  $f : M \rightarrow L$  is an  $R$ -homomorphism with  $f(N) = \{0_L\}$ , so that  $N \subseteq \ker f$ , then there is a unique homomorphism  $\bar{f} : M/N \rightarrow L$  such that  $f = \bar{f} \circ \text{can}$

**THEOREM 3.7.2** (First Isomorphism Theorem for Modules). Let  $R$  be a ring and let  $M, N$  be  $R$ -modules. Then every  $R$ -homomorphism  $f : M/\ker f \xrightarrow{\sim} \text{im} f$

## 4 Determinants and Eigenvalues Redux

### 4.1 The sign of a permutation

**DEFINITION 4.1.1.** The group of all permutations of the set  $\{1, 2, \dots, n\}$ , also known as bijections from  $\{1, 2, \dots, n\}$  to itself, is denoted by  $\mathfrak{S}_n$  and called the  $n$ -th **symmetric group**. It is a group under composition and it has  $n!$  elements.

A transposition is a permutation that swaps two elements of the set and leaves all the others unchanged.

**DEFINITION 4.1.2.** An inversion of a permutation  $\sigma \in \mathfrak{S}_n$  is a pair  $(i, j)$  such that  $1 \leq i < j \leq n$  and  $\sigma(i) > \sigma(j)$ . The number of inversions of the permutation  $\sigma$  is called the length of  $\sigma$  and written  $l(\sigma)$ . In formulas:

$$l(\sigma) = |\{(i, j) : i < j \text{ but } \sigma(i) > \sigma(j)\}|$$

The sign of  $\sigma$  is defined to be the parity of the permutations of  $\sigma$ . In formulas:

$$\text{sgn}(\sigma) = (-1)^{l(\sigma)}$$

**EXAMPLE 4.1.1.** consider  $(12453) = (12453)(6) \in \mathfrak{S}_6$ , the inversions are  $(1, 3), (2, 3), (2, 5), (4, 5)$ . therefore  $l((12453)) = 4$

**LEMMA 4.1.1** (Multiplicity of the sign). For each  $n \in \mathbb{N}$  the sign of a permutation produces a group homomorphism  $\text{sgn} : \mathfrak{S}_n \rightarrow \{+1, -1\}$  from the symmetric group to the two-element group of signs. In formulas:

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau) \quad \forall \sigma, \tau \in \mathfrak{S}_n$$

**DEFINITION 4.1.3.** For  $n \in \mathbb{N}$ , the set of even permutations in  $\mathfrak{S}_n$  forms a subgroup of  $\mathfrak{S}_n$  because it is the kernel of the group homomorphism  $\text{sgn} : \mathfrak{S}_n \rightarrow \{+1, -1\}$ . This group is the **alternating group** and is denoted  $A_n$

### 4.2 Determinants and What They Mean

**DEFINITION 4.2.1.** Let  $R$  be a commutative ring and  $n \in \mathbb{N}$ . The determinant is a mapping  $\det : \text{Mat}(n; R) \rightarrow R$  from square matrices with coefficients in  $R$  to the ring  $R$  from square matrices with coefficient in  $R$  to the ring  $R$  that is given by the following formula (**Leibniz formula**):

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \mapsto \det(A) = \sum_{\sigma \in \mathfrak{S}_n} \left( \text{sgn}(\sigma) \prod_{i=1}^n a_{i\sigma(i)} \right)$$

There is a really good demo in Example 4.2.3 in the Iain's note

**EXAMPLE 4.2.1.**

- An  $(n \times n)$  matrix  $A = (a_{ij})$  is upper triangular if  $a_{ij} = 0 \quad \forall i > j$ .  $\det(A) = \prod_{i=1}^n a_{ii}$
- The similar holds for the lower triangle

### 4.3 Characterising the Determinant

**DEFINITION 4.3.1.** Let  $U, V, W$  be  $F$ -vector spaces. A **bilinear form on  $U \times V$  with values in  $W$**  is a mapping  $H : U \times V \rightarrow W$  which is a linear mapping in both of its entries. This means that it must satisfy the following properties for all  $u_1, u_2 \in U$  and  $v_1, v_2 \in V$  and  $\lambda \in F$ :

$$\begin{aligned} H(u_1 + u_2, v_1) &= H(u_1, v_1) + H(u_2, v_1) \\ H(u_1, v_1 + v_2) &= H(u_1, v_1) + H(u_1, v_2) \\ H(\lambda u_1, v_1) &= \lambda H(u_1, v_1) \\ H(u_1, \lambda v_1) &= \lambda H(u_1, v_1) \end{aligned}$$

A bilinear form is **symmetric** if  $U = V$  and  $H(u, v) = H(v, u) \quad \forall u, v \in U = V$

A bilinear form is **altering** or **antisymmetric** if  $U = V$  and  $H(u, u) = 0 \quad \forall u \in U = V$

**DEFINITION 4.3.2.** Let  $V_1, \dots, V_n, W$  be  $F$ -vector spaces. A mapping  $H : V_1 \times V_2 \times \dots \times V_n \rightarrow W$  is a **multilinear form** aka. **multilinear** if for each  $j$  the mapping  $V_j$  defined by  $v_j \mapsto H(v_1, \dots, v_j, \dots, v_n)$  with the  $v_i \in V_i$  arbitrary fixed vectors of  $V_i$  for  $i \neq j$ , is linear. In the case  $n = 2$ . this is exactly the definition of a linear mapping.

**DEFINITION 4.3.3.** Let  $V$  and  $W$  be  $F$ -vector spaces. A multilinear form  $H : V \times \dots \times V \rightarrow W$  is **alternating** if it vanishes on every  $n$ -tuple of elements of  $V$  that has at least two entries equal, in order words:

$$(\exists i \neq j \text{ with } v_i = v_j \rightarrow H(v_1, \dots, v_j, \dots, v_i, \dots, v_n) = 0$$

In the case  $n = 2$ , this is exactly the definition of an alternating or antisymmetric bilinear mapping.

**THEOREM 4.3.1** (Characterisation of the Determinant). Let  $F$  be a field, The mapping  $\det : \text{Mat}(n; F) \rightarrow F$  is the unique alternating multilinear form on  $n$ -tuples of column vectors with values in  $F$  that takes the value  $1_F$  on the identity matrix.

### 4.4 Rules for Calculating with Determinants

**THEOREM 4.4.1** (Multiplicy for Calculating with Determinants). Let  $R$  be a commutative right and  $A, B \in \text{Mat}(n, R)$ . Then  $\det(AB) = \det(A)\det(B)$

**THEOREM 4.4.2** (Determinantal Criterion for invertibility). The determinant of a square matrix with entries in a field  $F$  is a non-zero i.f.f. the matrix is invertable.

**DEFINITION 4.4.1.** Let  $A \in \text{Mat}(n; R)$  for some commutative ring  $R$  and natural number  $n$ . Let  $i$  and  $j$  be integer between 1 and  $n$ . Then the  $(i, j)$  **cofactor** of  $A$  is  $C_{ij} = (-1)^{i+j} \det(A(i, j))$  where  $A(i, j)$  is the matrix  $A$  obtain from  $A$  deleting the  $i$ -th row and the  $j$ -th column.

**THEOREM 4.4.3** (Laplace's Expansion of the Determinant). Let  $A = (a_{ij})$  be an  $n \times n$ -matrix with entries from a commutative ring  $R$ . For a fixed  $i$  the  **$i$ -th row expansion of the determinant is**

$$\det(A) = \sum_{j=1}^n a_{ij} C_{ij} = \sum_{j=1}^n a_{ij} (-1)^{i+j} \det(A(i, j))$$

and for a fixed  $j$  in the  **$j$ -th column expansion of the determinant is**

$$\det(A) = \sum_{i=1}^n a_{ij} C_{ij} = \sum_{i=1}^n a_{ij} (-1)^{i+j} \det(A(i, j))$$

**DEFINITION 4.4.2** (Adjugate Matrix). Let  $A \in \text{Mat}(n; R)$  where  $R$  is a commutative ring. The **adjugate matrix**  $\text{adj}(A)$  is the  $(n \times n)$ -matrix whose entries are  $\text{adj}(A)_{ij} = C_{ij}$  where  $C_{ij}$  is the  $(i, j)$ -cofactor.

**THEOREM 4.4.4** (Cramer's Rule). Let  $A \in \text{Mat}(n; R)$  where  $R$  is a commutative ring. Then

$$A \cdot \text{adj}(A) = (\det A) I_n$$

**COROLLARY 4.4.1** (invertibility of Matrices). A square matrix with entries in a commutative ring  $R$  is invertible i.f.f. its determinant is a unit in  $R$ . That is,  $A \in \text{Mat}(n; R)$  is invertible i.f.f.  $\det(A) \in R^\times$ .

4.5 Eigenvalues and Eigenvectors

**DEFINITION 4.5.1.** Let  $f : V \rightarrow V$  an endomorphism of an  $F$ -vector space  $V$ . A scalar  $\lambda \in F$  is an eigenvalue of  $f$  i.f.f.  $\exists \vec{v} \in V \quad \vec{v} \neq \vec{0}$  such that  $f(\vec{v}) = \lambda \vec{v}$ . Each such vector is called an **eigenvector of  $f$  with eigenvalue  $\lambda$** . For any  $\lambda \in F$ , the **eigenspace of  $f$  with eigenvalue  $\lambda$**  is

$$E(\lambda, f) = \{ \vec{v} \in V : f(\vec{v}) = \lambda \vec{v} \}$$

**THEOREM 4.5.1** (Existance of Eigenvalues). Each endomorphism of a non-zero finite dimensional vector space over an algebraically closed field has an eigenvalue.

**DEFINITION 4.5.2.** Let  $R$  be a commutative ring and let  $A \in \text{Mat}(n; R)$  be a square matrix with entries in  $R$ . The polynomial  $\det(A - xI_n) \in R[x]$  is called the **characteristic polynomial of the matrix  $A$** . It is denoted by  $\chi_A(x) := \det(A - xI_n)$ .

Where  $\chi$  stands for  $\chi$ aracteristic(Okay Iain you're a good dad for sure...).

**THEOREM 4.5.2** (Eigenvalues and Characteristic Polynomials). Let  $F$  be a field and  $A \in \text{Mat}(n; F)$  with entries in  $F$ . The eigenvalues of the linear mapping  $A : F^n \rightarrow F^n$  are exactly the roots of the characteristic polynomial  $\chi_A$ .

4.6 Triangularisable, Diagonalisable, and the Cayley-Hamilton Theorem

Iain (not Ian just to be clear) said he's not examing triangularisable. (Will FC)

**PROPOSITION 4.6.1** (Triangularisability). Let  $f : V \rightarrow V$  be an endomorphism of a finite dimensional  $F$ -vector space  $V$ . The following two statements are equivalent:

- 1. The vector space  $V$  has an ordered basis  $\mathcal{B} = (\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n)$  such that

$$\begin{aligned} f(\vec{v}_1) &= a_{11} \vec{v}_1 \\ f(\vec{v}_2) &= a_{12} \vec{v}_1 + a_{22} \vec{v}_2 \\ &\vdots \\ f(\vec{v}_n) &= \sum_{i=1}^n a_{in} \vec{v}_i \in V \end{aligned}$$

such that the  $n \times n$  matrix  ${}_B[f]_B = (a_{ij})$  representing  $f$  with respect to  $\mathcal{B}$  is upper triangular

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

When this happens, we say that  $f$  is **triangularisable**.

- 2. The characteristic polynomial  $\chi_f(x)$  of  $f$  decomposes into linear factors in  $F[x]$ .

**DEFINITION 4.6.1** (Diagonalisibility). Aa endomorphism  $f : V \rightarrow V$  of an  $F$ -vector space  $V$  is **diagonalisable** i.f.f.  $\exists$  basis of  $V$  consisting of eigenvectors of  $f$ . If  $V$  is finite dimensional then this is the same as saying that  $\exists$  an order basis  $\mathcal{B} = \{\vec{v}_1, \dots, \vec{v}_n\}$  such that corresponding matrix representing  $f$  is diagonal, that is  ${}_B[f]_B = \text{diag}(\lambda_1, \dots, \lambda_b)$ . In this case,  $f(\vec{v}_1) = \lambda_1 \vec{v}_1$ .

A square matrix is **diagonalisable** i.f.f. the corresponding linear mapping  $F^n \rightarrow F^n$  given by left multiplication by  $A$  is diagonalisable. This means  $\exists$  invertable matrix  $P \in \text{GL}(n; F)$  such that  $P^{-1}AP = \text{diag}(\lambda_1, \dots, \lambda_n)$

**LEMMA 4.6.1** (Linear Independence of Eigenvectors). Let  $f : V \rightarrow V$  be an endomorphism of a vector space  $V$  and let  $\vec{v}_1, \dots, \vec{v}_n$  be eigenvectors of  $f$  with pairwise different eigenvalues  $\lambda_1, \dots, \lambda_n$ . Then the vectors are linearly independent.

**THEOREM 4.6.1** (Cayley-Hamilton Theorem). Let  $A \in \text{Mat}(n; R)$  be a square matrix with entries in a commutative ring  $R$ . The evaluating its characteristic polynomial  $\chi_A(x) \in R[x]$  at the matrix  $A$  gives zero.

4.7 Google's PageRank Algorithm (Markov matrix/stochastic matrix)

**DEFINITION 4.7.1.** A matrix  $M$  whose entries are non-zero and such that the sum of the entries of each column equal 1 is a **Markov matrix** or a **stochastic matrix**.

**LEMMA 4.7.1.** Suppose  $M \in \text{Mat}(n; \mathbb{R})$  is a Markov matrix. Then 1 is an eigenvalue of  $M$

**THEOREM 4.7.1** (Perron, 1907). If  $M \in \text{Mat}(n; \mathbb{R})$  is a Markov matrix all whose entries are positive, then eigenspace  $E(1, M)$  is one dimensional. There exists a unique basis vector  $\vec{v} \in E(1, M)$  all of whose entries are positive real numbers,  $v_i > 0$  for all  $i$ , and such that the sum of it entries is 1,  $\sum_i v_i = 1$

5 Inner Product Spaces

5.1 Inner Product Space: Definitions

**DEFINITION 5.1.1.** Let  $V$  be a vector space over  $\mathbb{R}$ . An **inner product** on  $V$  is a mapping  $(-, -) : V \times V \rightarrow \mathbb{R}$  that satisfies the following  $\forall \vec{x}, \vec{y}, \vec{z} \in V$  and  $\lambda, \mu \in \mathbb{R}$ :

- 1.  $(\lambda \vec{x} + \mu \vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})$
- 2.  $(\vec{x}, \vec{y}) = (\vec{y}, \vec{x})$
- 3.  $(\vec{x}, \vec{x}) \geq 0$ , with  $\vec{x} = \vec{0} \Leftrightarrow (\vec{x}, \vec{x}) = 0$

A **real innter space product space** is a real vector space endowed with an inner product.

**EXAMPLE 5.1.1.**

- A dot product is a statdard inner product

**DEFINITION 5.1.2.** Let  $V$  be a vector space over  $\mathbb{C}$ . An **inner product** on  $V$  is a mapping  $(-, -) : V \times V \rightarrow \mathbb{C}$  that satisfies the following  $\forall \vec{x}, \vec{y}, \vec{z} \in V$  amdd  $\lambda, \mu \in \mathbb{C}$ :

- 1.  $(\lambda \vec{x} + \mu \vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})$
- 2.  $(\vec{x}, \vec{y}) = \overline{(\vec{y}, \vec{x})}$
- 3.  $(\vec{x}, \vec{x}) \geq 0$

Where  $\bar{z}$  denotes the complex conjugate of  $z$  A **complex innter space product space** is a complex vector space endowed with an inner product.

**EXAMPLE 5.1.2.**

- **Standard inner product:**  $(\vec{v}, \vec{w}) = \sum_{i=1}^n (v_i \bar{w}_i)$

**DEFINITION 5.1.3.** In a real or complex innter product space the **length** or **inner product norm** or **norm**  $\|\vec{v}\| = \sqrt{(\vec{v}, \vec{v})}$ . Vectors whose length is 1 are called **units**. Two vectors  $\vec{v}, \vec{w}$  are **orthogonal** can be denoted as  $\vec{v} \perp \vec{w}$  i.f.f.  $\vec{v}, \vec{w} = 0$

**DEFINITION 5.1.4.** A family  $(\vec{v}_i)_{i \in I}$  for vectors from an inner product space is an **orthogonal family** if all the vectors  $\vec{v}_i$  have length 1 and if they are pairwise orthogonal to each other, which, using the *Kronecker delta symbol* defined in Example 2.1.2(Check full note), means  $(\vec{v}_i, \vec{v}_j) = \delta_{ij}$   
An orthogonal family that is a basis is an **orthogonal basis**

**THEOREM 5.1.1.** Every finite dimensional inner product space has an orthonormal basis



5.2 Orthogonal Complements and Orthogonal Projections

**DEFINITION 5.2.1.** Let  $V$  be an inner product space and let  $T \subseteq V$  be an arbitrary subset. Define  $T^\perp = \{\vec{v} \in V : \vec{v} \perp \vec{t} \ \forall \vec{t} \in T\}$  calling this set the **orthogonal** to  $T$

**PROPOSITION 5.2.1.** Let  $V$  be an inner product space and let  $U$  be a finite dimensional subspace of  $V$ . Then  $U$  and  $U^\perp$  are complementary in the sense of definition 1.7.6 (Check full note). In other words  $V = U \oplus U^\perp$

**DEFINITION 5.2.2.** Let  $U$  be a finite dimensional subspace of an inner product space  $V$ . The space  $U^\perp$  is the **orthogonal Complement to  $U$** . The **orthogonal projection from  $V$  to  $U$**  is the mapping  $\pi_U : V \rightarrow V$  that sends  $\vec{v} = \vec{p} + \vec{r}$  to  $\vec{p}$

**PROPOSITION 5.2.2.** Let  $U$  be a finite dimensional subspace of an inner product space  $V$  and let  $\pi_U$  be the orthogonal projection from  $V$  onto  $U$ .

- 1.  $\pi_U$  is a linear mapping with  $\text{im}(\pi_U) = U$  and  $\text{ker}(\pi_U) = U^\perp$
- 2. If  $\{\vec{v}_1, ..., \vec{v}_n\}$  is an orthogonal basis of  $U$ , then  $\pi_U$  is given by the following formula for all  $\vec{v} \in V$

$$\pi_U(\vec{v}) = \sum_{i=1}^n (\vec{v}, \vec{v}_i) \vec{v}_i$$

- 3.  $\pi_U^2 = \pi_U$ , that is  $\pi_U$  is an **idempotent**

**THEOREM 5.2.1** (Cauchy-Schwarz Inequality). Let  $\vec{v}, \vec{w}$  be vectors in an inner product space. Then  $|(\vec{v}, \vec{w})| \leq \|\vec{v}\| \|\vec{w}\|$  with equality i.f.f.  $\vec{v}, \vec{w}$  are linearly dependent.

**COROLLARY 5.2.1.** The norm  $\|\cdot\|$  on an inner product space  $V$  satisfies, for any  $\vec{v}, \vec{w} \in V$  and scalar  $\lambda$ :

- 1.  $\|\vec{v}\| \geq 0$  with equality i.f.f.  $\vec{v} = \vec{0}$
- 2.  $\|\lambda \vec{v}\| = |\lambda| \|\vec{v}\|$
- 3.  $\|\vec{v} + \vec{w}\| \leq \|\vec{v}\| + \|\vec{w}\|$  (triangle inequality)

**THEOREM 5.2.2** (Gram-Schmit Process). Let  $\vec{v}_1, ..., \vec{v}_k$  be a linearly independent vectors in an inner product space  $V$ . Then there exists an orthonormal family  $\vec{w}_1, ... \vec{w}_k$  with the property for all  $1 \leq i \leq k$ :

$$\vec{w}_i \in \mathbb{R}_{>0} \vec{v}_i + \langle \vec{v}_1 - \vec{1}, ..., \vec{v}_1 \rangle$$

Therefore,  $\forall i \in [1, k] \in \mathbb{N} \exists \vec{\lambda}$  s.t.  $\exists \vec{w}_i = \vec{v}_i - \sum_{j=1}^{i-1} \lambda_j \vec{v}_j$

5.3 Adjoints and Self-Adjoint

**DEFINITION 5.3.1.** Let  $V$  be an inner product space. Then two endomorphism  $T, S : V \rightarrow V$  are called **adjoint** to the other if the following holds for all  $\vec{v}, \vec{w} \in V$ :

$$(T\vec{v}, \vec{w}) = (\vec{v}, S\vec{w})$$

In this say we can express  $S = T^*$  and call  $S$  the adjoint of  $T$ . If  $S = T^*$  then  $T = S^*$

**THEOREM 5.3.1.** Let  $V$  be a finite dimensional inner product space. Let  $T : V \rightarrow V$  be an endomorphism. Then  $T^*$  exists. That is,  $\exists$  a unique linear mapping  $T^* : V \rightarrow V$  such that for all  $\vec{v}, \vec{w} \in V$

$$(T\vec{v}, \vec{w}) = (\vec{v}, T^* \vec{w})$$

**DEFINITION 5.3.2.** An endomorphism of an inner product space  $T : V \rightarrow V$  is **self adjoint** if  $T^* = T$

**THEOREM 5.3.2.** Let  $T : V \rightarrow V$  be a self-adjoint linear mapping on an inner product space  $V$ .

- 1. Every eigenvalue of  $T$  is real.
- 2. If  $\lambda$  and  $\mu$  are distinct eigenvalues of  $T$  with corresponding eigenvectors  $\vec{v}, \vec{w}$ , then  $(\vec{v}, \vec{w}) = 0$
- 3.  $T$  has an eigenvalue

**THEOREM 5.3.3** (The Spectral Theorem for Self-Adjoint Endomorphisms). Let  $V$  be a finite dimensional inner product space and let  $T : V \rightarrow V$  be a self-adjoint linear mapping. Then  $V$  has an orthonormal basis consisting of eigenvectors of  $T$

**DEFINITION 5.3.3** (Orthogonal Matrix). An **orthogonal matrix** is a square matrix  $P$  with real entries such that  $P^{-1} = P^T$

**DEFINITION 5.3.4.** The **orthogonal group** is defined  $O(n) = \{P \in \text{Mat}(n; \mathbb{R}) : P^T P = I_n\}$

**COROLLARY 5.3.1** (The Spectral Theorem for Real Symmetric Matrices). Let  $A$  be a real  $(n \times n)$ -symmetrical matrix. Then  $\exists$  an  $(n \times n)$ -orthogonal matrix  $P$  such that

$$P^T A P = P^{-1} A P = \text{diag}(\lambda_1, ..., \lambda_n)$$

Where  $\lambda_1, ..., \lambda_n$  are the (necessarily real) eigenvalues of  $A$ , repeated according to their multiplicity as roots of the characteristic polynomial of  $A$

**DEFINITION 5.3.5** (Unitary Matrix). An **unitary matrix** is an  $(n \times n)$ -matrix  $P$  with complex entries such that  $\overline{P}^T P = I_n$ . In other words,  $P^{-1} = \overline{P}^T$

**COROLLARY 5.3.2** (The Spectral Theorem for Hermitian Matrices). Let  $A$  be a  $(n \times n)$ -hermitian matrix. Then there is an  $(n \times n)$ -unitary matrix  $P$  such that

$$\overline{P}^T A P = P^{-1} A P = \text{diag}(\lambda_1, ..., \lambda_n)$$

Where  $\lambda_1, ..., \lambda_n$  are the (necessarily real) eigenvalues of  $A$ , repeated according to their multiplicity as roots of the characteristic polynomial of  $A$

6 Jordan Normal Form

Will not be incuded in Exam yay

## Quick References

- **Abelian Group:** For group in with operation  $(A, *)$  to be abelian group, the following has to be fulfilled:
  1. **Closure:**  $\forall a, b \in A, a * b \in A$
  2. **Associativity:**  $\forall a, b, c \in A, (a * b) * c = a * (b * c)$
  3. **Identity:**  $\exists e \in A$  s.t.  $e * a = a * e = a \forall a \in A$
  4. **Inverse:**  $\forall a \in A \exists a^{-1}$  **s.t.**  $a^{-1} * a = a * a^{-1} = e$
  5. **Communtativity:**  $\forall a, b \in A, a * b = b * a$
- **Change of Basis:** for standard basis  $A = \{\vec{v_1}, ..., \vec{v_n}\}$  and basis  $B = \{(\sum_{i=1}^n a_{i1}\vec{w_i}), ..., (\sum_{i=1}^n a_{in}\vec{w_i})\}$ ,

$${}_A[id]_B = (a_{ij})$$

The blah-morphism table

blah-morphism	Linear?	Bijective?	$f : V \rightarrow V?$
Homomorpghism	Yes	Not-required	Not-required
Isomorphism	Yes	Yes	Not-required
Endomorphism	Yes	Not-required	Yes
Automorphism	Yes	Yes	Yes