Honours Algebra
Quick Notes

Ian S.W. Ma

Contents

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 $\alpha_1, ..., \alpha_n \in F$:

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

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*"

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

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:

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

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

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

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 $a_i j$ 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:

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

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 $\Phi_{\mathcal{A}} \overset{\sim}{\to} V, (\alpha_a, ..., \alpha_m)^T \mapsto \sum_{i=1}^{m} \alpha_i \overrightarrow{v}_i$ 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:

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

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 $\cdot$: $R \times R \to R$ is assosiative and that there is an **identity element** $1 = 1_R \in R$, often called just the **identity**, with the peoperty that $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$
3. The Distributive laws hold, meaning that for all $a, b, c \in R$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \textbf{addition}$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \quad \textbf{multiplication}$$

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 (Divisbility by Sum)**.** A natural number is divisible by 3(respectively by 9) percisely 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 Peoperties of Rings

LEMMA 3.2.1 (Mutiplying 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. $(-a)(-b) = ab$

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 3.2.1. 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 3.2.2 (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 $ba = 0$

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

DEFINITION 3.2.3 (Integral domain)**.** An **integral domain** is a non-zero commutative ring that has no zero-divisors, therefore the 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. 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 **fnite** integral domain is a field

3.3 Polynomials

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

$$P = a_0 + a_1 X + a_2 X^2 + ... + a_m X^m$$

for some $m \in \mathbb{N} \backslash 0$ and elements $a_i \in R$ for $0 \leq i \leq m$. The set of all Polynomials over R is denoted by $R[X]$. Incase 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, quardratic for a_2, then cubic for a_3.

DEFINITION 3.3.2. Whith 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 indentity 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 $R[X]$

THEOREM 3.3.1 (Division and Remainder)**.** Let R be an integral domain and let $P, Q \in R[X]$ with Q. Then there 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 X in the polynomial P by the corresponding powers of λ. In this way we have a mapping $R[X] \to \text{Maps}(R, R)$
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 $P(\lambda) = 0$

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

THEOREM 3.3.2 (Fundamental Theorem of Algebra)**.** The field of complex numbers $\mathbb{C}$, is algebraically closed.

THEOREM 3.3.3. If F is an algebraically closed field, then every non-zero polynomial $P \in F[X] \backslash \{0\}$ **decomposes into linear factors**

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

with $n \geq 0, c \in F^{\times}$ and $\lambda_1, ..., \lambda_n \in F$

3.4 Homomorpgism, Ideals and Subrings

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

$$f(x+y) = f(x)f(y)$$
$$f(xy) = f(x)f(y)$$

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

1. $f(0_r) =)_s$ Where $O_R, 0_S$ 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. $I \neq 0$
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 $T \subset R$. The the **ideal of R generated by T** is the set

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

PROPOSITION 3.4.1. Let R be a commutative ring and let $T \subseteq R$. The ${}_R\langle T \rangle$ 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 $f : R \to S$ be a ring homomorphism. Since f is in particular a group homomorphism. Then $\ker(f)$ is an ideal of R

LEMMA 3.4.2. f us 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

PROPOSITION 3.4.2 (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: $a, b \in R' \to a - b \in R'$, and
3. R' is closed under multiplication

PROPOSITION 3.4.3. Let R and S be subrings and $f : R \to S a ring homomorphism$

1. If R' is a subring of R then $f(R')$ is a subring of S. In particular, $\mathrm{im}(f)$ 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 $f|_{R^\times} : R^\times \to S^\times$

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, adn only in theis 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**: $(xRy \cap yRx) \to xRz$

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

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

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

3.6 Factor Rings and the First Isomorphism Theorem

DEFINITION 3.6.1. 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 additionis defined by

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

and multiplication is defined by

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

THEOREM 3.6.2 (First Isomorphism Theorem for Rings)**.** Let R and S be rings. Then every ring homomorphism $f : R \longrightarrow S$ induces a ring isomorphism

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

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

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

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 $f : M \to N$ is an R-**homomorphism** or **homomorphism** if the following hold for all $a, b \in M$ and $r \in R$

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

The kernel of f is $\ker f = \{a \in M : f(a) =)_N\} \subseteq M$ and the image of f is $\mathrm{im} f = \{f(a) : a \in M\} \subseteq N$. 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 $f : M \to N$ be an R-homomorphism. The $\ker f$ is a submodule of M and $\mathrm{im} f$ is a submodule of N.

LEMMA 3.7.3. Let R be a ring, M, N be R-modules and let $f : M \to N$ 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

$$_R\langle T\rangle = \{r_1t_1 + ... + r_mt_m : t_1, ..., t_m \in T, r_1, .., r_m \in R\}$$

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

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 $f : M/\ker f \xrightarrow{\sim} \mathrm{im} f$

4 Determinants and Eigenvalues Redux

4.1 The sign of a permutation

DEFINITION 4.1.1. The group of all permutations of the set $\{1, 2, ..., n\}$, also known as bijections from $\{1, 2, ..., n\}$ to itself, is denoted by $\mathfrak{S}_\mathfrak{n}$ 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 apair (i, j) such that $1 \leq i < j \leq n$ and $\sigma(i) > \sigma(j)$. The number of inversions of the permutation σ is called the length of σ ans written $l(\sigma)$. In formulas:

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

The sign of σ is defined to be the parity of the permutations of σ. In formulas:

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

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

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

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 $\mathbf{sgn} : \mathfrak{S}_n \to \{+1, -1\}$. This group is the **alterating 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 $\det : \text{Mat}(n; R) \to R$ from square matrices with coefficients in R to the ring R from square matrices with coefficient in R ot the ring R that is given by the following formula (**Leibniz formula**):

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

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 $H : U \times V \to W$ 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 $V_1, ..., V_n, W$ be F-vector spaces. A mapping $H : V_1 \times v_2 \times ... \times V_n \to W$ is a **multilinear form** or just **multilinear** if for each j the mapping V_j defined by $v_j \mapsto H(v_1, ..., v_j, ..., v_n)$ with the $v_i \in V_i$ arbitrary fixed vectors pf 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 $H : V \times ... \times V \to W$ is **alterating** if it vanishes on every n-tuple of elements of V that has at least two entries equal, in order words if:

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

THEOREM 4.3.1 (Characterisation of the Determinant)**.** Let F be a field, The mapping $\det : \mathrm{Mat}(n; F) \to F$ is the alterating 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 Caluculating with Determinants

THEOREM 4.4.1 (Multiplicy for Calculating with Determinants)**.** Let R be a commutative right and $A, B \in \mathrm{Mat}(n, R)$. 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 $A \in \mathrm{Mat}(n; R)$ fir 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 $C_{ij} = (-1)^{i+j}\det(A\langle i, j\rangle)$ where $A\langle i, j\rangle$ is the matrix I 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 form a commutative ring R. For a fixed i the **i-th row expansion of the determinant is**

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

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

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

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

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

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

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, $A \in Mat(n; R)$ is invertible i.f.f. $det(A) \in R^{\times}$.

4.5 Eigenvalues and Eigenvectors

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

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

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.