

Honours Algebra

Quick Notes

Ian S.W. Ma

Contents

1	Vector Spaces	1
1.1	Solution of Simultaneous Linear Equations	1
1.2	Fields and Vector Spaces	1
1.3	Product of Sets and of Vector Spaces	2
1.4	Vector Subspaces	2
1.5	Linear Independence and Bases	3
1.6	Dimension of a vector space	4
1.7	Linear Mappings	5
1.8	Rank-Nullity Theorem	5
2	Linear Mappings and Matrices	6
2.1	Linear Mappings $F^m \rightarrow F^n$ and Matrices	6
2.2	Basic Properties of Matrices	6
2.3	Abstract Linear Mappings and Matrices	7
2.4	Change of Matrix by Change of Basis	8
3	Rings and Modules	8
3.1	Rings	8
3.2	Properties of Rings	9
3.3	Polynomials	10
3.4	Homomorphism, Ideals and Subrings	11
3.5	Equivalence Relations	12
3.6	Factor Rings and the First Isomorphism Theorem	12

1 Vector Spaces

1.1 Solution of Simultaneous Linear Equations

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

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

is a **system of linear Equations**

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

1.2 Fields and Vector Spaces

DEFINITION 1.2.1.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.3 Product of Sets and of Vector Spaces

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

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

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

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

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

1.4 Vector Subspaces

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

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

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

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

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

1.5 Linear Independence and Bases

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

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

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

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

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

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

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

is a bijection

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

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

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

THEOREM 1.5.1. Let V be a vector space.

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

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

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

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

1.6 Dimension of a vector space

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

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

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

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

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

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

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

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

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

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

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

1.7 Linear Mappings

DEFINITION 1.7.1. Let V, W be a vector spaces over a field F . A mapping $f : V \rightarrow W$ is called **linear** or more percisely **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 bwtween 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 br a mapping is called a **fixed point** of the mapping. Given a mapping $f : X \rightarrow X$, 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

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

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

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

1.8 Rank-Nullity Throrem

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 if V

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

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

2 Linear Mappings and Matrices

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

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

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

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

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

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

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

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

2.2 Basic Properties of Matrices

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

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 invertible 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 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 $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_m)$ and $\mathcal{B} = (\vec{w}_1, \dots, \vec{w}_n)$. Then to each linear mapping $f : V \rightarrow W$ we associate bases 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 $\Phi_{\mathcal{A}} : V \xrightarrow{\sim} \sum_{i=1}^m \alpha_i \vec{v}_i$ 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:

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

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

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

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 ${}_B[f]_{\mathcal{A}}$ 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:

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

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 $a, b, c \in R$

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

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

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 (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. $(-a)(-b) = ab$

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 $ba = 0$

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

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 **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 $R[X]$

THEOREM 3.3.1 (Division and Remainder). Let R be an integral domain and let $P, Q \in R[X]$ with $Q \neq 0$. 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 λ . In this way we have a mapping $R[X] \rightarrow \text{Maps}(R, R)$

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

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 3.3.2 (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 $P \in F[X] \setminus \{0\}$ **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 Homomorphism, 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 respective 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 $T \subset R$. The **ideal of R generated by T** is the set

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

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 $f : R \rightarrow S$ 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 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

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: $a, b \in R' \rightarrow a - b \in R'$, and
3. R' is closed under multiplication

PROPOSITION 3.4.3. 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 Equivalence 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 precisely one element from each equivalence class 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. $g : (X/\sim) \rightarrow Z$ is **well-defined** if \exists a mapping $f : X \rightarrow Z$ such that f has the property $x \sim y \rightarrow f(x) = f(y) \cap g = \bar{f}$

3.6 Factor Rings and the First Isomorphism Theorem