

Honours Algebra Notes

Anthony Catterwell

March 17, 2019

Contents

1	Vector Spaces	2
1.1	Solutions of simultaneous linear equations	2
1.2	Fields and vector spaces	2
1.3	Products of sets and of vector spaces	3
1.4	Vector subspaces	3
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	6
2	Linear Mappings and Matrices	6
2.1	Linear mappings $F^m \rightarrow F^n$ and matrices	6
2.2	Basic properties of matrices	7
2.3	Abstract linear mappings and matrices	8
2.4	Change of a matrix by change of basis	8
3	Rings and Modules	9
3.1	Rings	9
3.2	Properties of rings	9
3.3	Polynomials	10
3.4	Homomorphisms, Ideals, and Subrings	11
3.5	Equivalence Relations	13
3.6	Factor Rings and the First Isomorphic Theorem	13
3.7	Modules	14
4	Determinants and Eigenvalues Redux	16
4.1	The sign of a permutation	16
5	Reference	17
5.1	Terminology of Algebraic Structures	17

1 Vector Spaces

1.1 Solutions of simultaneous linear equations

- **Theorem 1.1.4** *Solution sets of inhomogeneous systems of linear equations*

If the solution set of a linear system of equations is non-empty, then we obtain all solutions by adding component-wise an arbitrary solution of the associated homogenised system to a fixed solution of the system.

1.2 Fields and vector spaces

- **Definition 1.2.1.1** *Fields*

A *field* F is a set with functions

$$\begin{aligned}\text{addition} &= + : F \times F \rightarrow F ; (\lambda, \mu) \mapsto \lambda + \mu \\ \text{multiplication} &= \cdot : F \times F \rightarrow F ; (\lambda, \mu) \mapsto \lambda\mu\end{aligned}$$

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

$$\lambda + \mu = \mu + \lambda, \lambda \cdot \mu = \mu \cdot \lambda, \lambda + 0_F = \lambda, \lambda \cdot 1_F = \lambda \in F, \quad \forall \lambda, \mu \in F$$

For every $\lambda \in F$ there exists $-\lambda \in F$ such that

$$\lambda + (-\lambda) = 0_F \in F$$

For every $\lambda \neq 0 \in F$ there exists $\lambda^{-1} \neq 0 \in F$ such that

$$\lambda(\lambda^{-1}) = 1_F \in F$$

- **Definition 1.2.1.2** *Vector space*

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

$$F \times V \rightarrow V : (\lambda, \mathbf{v}) \mapsto \lambda\mathbf{v}$$

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

$$\begin{aligned}\lambda(\mathbf{v} + \mathbf{w}) &= (\lambda\mathbf{v}) + (\lambda\mathbf{w}) && \text{(distributivity)} \\ (\lambda + \mu)\mathbf{v} &= (\lambda\mathbf{v}) + (\mu\mathbf{v}) && \text{(distributivity)} \\ \lambda(\mu\mathbf{v}) &= (\lambda\mu)\mathbf{v} && \text{(associativity)} \\ 1_F\mathbf{v} &= \mathbf{v}\end{aligned}$$

A vector space V over a field F is called an F -*vector space*.

- **Lemma 1.2.2** *Product with the scalar zero*

If V is a vector space and $\mathbf{v} \in V$, then $0\mathbf{v} = \mathbf{0}$

- **Lemma 1.2.3** *Product with the scalar (-1)*

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

- **Lemma 1.2.4** *Product with the zero vector*

If V is a vector space over a field F , then $\lambda\mathbf{0} = \mathbf{0}$ for all $\lambda \in F$. Furthermore, if $\lambda\mathbf{v} = \mathbf{0}$, then either $\lambda = 0$ or $\mathbf{v} = \mathbf{0}$.

1.3 Products of sets and of vector spaces

1.4 Vector subspaces

- **Definition 1.4.1** *Vector subspaces*

A subset U of a vector space V is called a *vector subspace* or *subspace* if U contains $\mathbf{0}$ and

$$\mathbf{u}, \mathbf{v} \in U \text{ and } \lambda \in F \implies \mathbf{u} + \mathbf{v} \in U \text{ and } \lambda \mathbf{u} \in U$$

- **Proposition 1.4.5** Generating a vector subspace from a subset

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

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

It can be described as the set of all vectors $\alpha_1 \mathbf{v}_1 + \cdots + \alpha_r \mathbf{v}_r$ with $\alpha_1, \dots, \alpha_r \in F$ and $\mathbf{v}_1, \dots, \mathbf{v}_r \in T$, together with $\mathbf{0}$ in the case $T = \emptyset$.

- **Definition 1.4.7** *Generating set*

A subset of a vector space is called a *generating set* of our vector space if its span is all of the vector space. A vector space that has a finite generating set is said to be *finitely generated*.

- **Definition 1.4.9**

The set of all subsets $\mathcal{P}(X) = \{U : U \subseteq X\}$ of X is the *power set* of X .

A subset of $\mathcal{P}(X)$ is 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 sets of our system \mathcal{U} :

$$\begin{aligned} \bigcup_{U \in \mathcal{U}} U &= \{x \in X : \exists U \in \mathcal{U}. x \in U\} \\ \bigcap_{U \in \mathcal{U}} U &= \{x \in X : x \in U \forall U \in \mathcal{U}\} \end{aligned}$$

In particular the intersection of the empty system of subsets of X is X , and the union of the empty system of subsets X is the empty set.

1.5 Linear independence and bases

- **Definition 1.5.1** *Linear independence*

A subset L of a vector space V is *linearly independent* if for all pairwise different vectors $\mathbf{v}_1, \dots, \mathbf{v}_r \in L$ and arbitrary vectors $\alpha_1, \dots, \alpha_r \in F$,

$$\alpha_1 \mathbf{v}_1 + \cdots + \alpha_r \mathbf{v}_r = \mathbf{0} \implies \alpha_1 = \cdots = \alpha_r = 0$$

- **Definition 1.5.2** *Linear dependence*

A subset L of a vector space V is called *linearly dependent* if it is not linearly independent.

- **Definition 1.5.8** *Basis*

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

- **Theorem 1.5.11** Linear combinations of basis elements

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

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

is a bijection.

- **Theorem 1.5.12** Characterisation of bases

The following are equivalent for a subset E of a vector space V :

1. E is a basis, i.e. a linearly independent generating set;
2. E is minimal among all generating sets, meaning that $E \setminus \{\mathbf{v}\}$ does not generate V , $\forall \mathbf{v} \in E$;
3. E is maximal among all linearly independent subsets, meaning that $E \cup \{\mathbf{v}\}$ is not linearly independent $\forall \mathbf{v} \in V$.

- **Corollary 1.5.13** The existence of a basis

Let V be a finitely generated vector space over a field F . The V has a basis.

- **Theorem 1.5.14** (Useful variant on the Characterisation of bases)

Let V be a vector space.

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

- **Definition 1.5.15**

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 point-wise addition and multiplication by a scalar. The subset of all mappings which send almost all elements of X to zero is a vector subspace

$$F\langle X \rangle \subseteq \text{Maps}(X, F)$$

This vector subspace is called the *free vector space on the set X* .

- **Theorem 1.5.16** (Useful variant on Linear combinations of basis elements)

Let F be a field, V an F -vector space, and $(\mathbf{v}_i)_{i \in I}$ a family of vectors from the vector space V . The following are equivalent:

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

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

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, $L \subset V$ finite linearly independent subset, and $E \subseteq V$ generating set. Then there is an injection $\Phi : L \rightarrow E$ such that $(E \setminus \Phi(L)) \cup L$ is also a generating set for V .

We can swap out some elements of a generating set by the elements of our linearly independent set, and still keep a generating set.

- **Lemma 1.6.3** 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 $\mathbf{w} \in V \setminus M$ is a vector set not belonging to M such that $M \cup \{\mathbf{w}\}$ is linearly independent, then there exists $\mathbf{e} \in E \setminus M$ such that $\{E \setminus \{\mathbf{e}\}\} \cup \{\mathbf{w}\}$ is a generating set for V .

- **Corollary 1.6.4** Cardinality of bases

Let V be a finitely generated vector space.

1. V has a finite basis;
2. V cannot have an infinite basis;
3. Any two bases of V have the same number of elements.

- **Definition 1.6.5** *Dimension*

The cardinality of one (and each) basis of a finitely generated vector space V is called the *dimension* of V and is denoted $\dim V$. If the vector space is not finitely generated, then $\dim V = \infty$ and V is *infinite dimensional*.

- **Corollary 1.6.8** Cardinality criterion for bases

Let V be a finitely generated vector space.

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

- **Corollary 1.6.9** Dimension estimate for vector subspaces

A proper vector subspace of a finite dimensional vector space has itself a strictly smaller dimension.

- **Theorem 1.6.11** The dimension theorem

Let V be a 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** Linear mappings

Let V, W be vector spaces over a field F . A mapping $f : V \rightarrow W$ is called *linear* if for all $\mathbf{v}_1, \mathbf{v}_2 \in V$ and $\lambda \in F$ we have

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

A bijective linear mapping is called an *isomorphism* of vector spaces. If there is an isomorphism of vector spaces, we call them *isomorphic*. A homomorphism from one vector space to itself is called an *endomorphism*. An isomorphism of a vector space to itself is called an *automorphism*.

- **Definition 1.7.5** *Fixed point*

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 1.7.6** *Complementary*

Two vector subspaces V_1, V_2 of a vector space V are *complementary* if addition defines a bijection

$$V_1 \times V_2 \rightarrow V$$

- **Theorem 1.7.7** 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 if and only if it has dimension n .

- **Lemma 1.7.8** 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

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

In other words, each linear mapping determines and is completely determined by the values it takes on a basis.

- **Proposition 1.7.9**

1. Every injective linear mapping $f : V \rightarrow W$ has a *left inverse*, in other words a linear mapping $g : W \rightarrow V$ such that $g \circ f = \text{id}_V$
2. Every surjective linear mapping $f : V \rightarrow W$ has a *right inverse*, in other words a linear mapping $g : W \rightarrow V$ such that $f \circ g = \text{id}_W$

1.8 Rank-Nullity theorem

- **Definition 1.8.1**

The *image* of a linear mapping $f : V \rightarrow W$ is the subset $\text{im}(f) = f(V) \subseteq W$. It is a vector subspace of W . The pre-image of the zero vector of a linear mapping $f : V \rightarrow W$ is denoted by

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

and is called the *kernel* of the linear mapping f . The kernel is a vector subspace of V .

- **Lemma 1.8.2**

A linear mapping $f : V \rightarrow W$ is injective if and only if $\ker f = 0$.

- **Theorem 1.8.4** Rank-Nullity theorem

Let $f : V \rightarrow W$ be a linear mapping between vector spaces. Then

$$\begin{aligned}\dim V &= \dim(\ker f) + \dim(\text{im} f) \\ &= \text{nullity} + \text{rank}\end{aligned}$$

- **Corollary 1.8.5** (Dimension theorem, again)

Let V be a vector space, and $U, W \subseteq V$ vector subspaces. Then

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

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 $m, n \in \mathbb{N}$. 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

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

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

$$[f] \equiv (f(\mathbf{e}_1) | f(\mathbf{e}_2) | \cdots | f(\mathbf{e}_m))$$

- **Definition 2.1.6** *Product*

Let $n, m, l \in \mathbb{N}$, F and 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

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

Matrix multiplication produces a mapping

$$\begin{aligned} \text{Mat}(n \times m; F) \times \text{Mat}(m \times l; F) &\rightarrow \text{Mat}(n \times l; F) \\ (A, B) &\mapsto AB \end{aligned}$$

- **Theorem 2.1.8** Composition of linear mappings and products of matrices

Let $g : F^l \rightarrow F^m$ and $f : F^m \rightarrow F^n$ be linear mappings. The representing matrix of their composition is the product of their representing matrices

$$[f \circ g] = [f] \circ [g]$$

- **Proposition 2.1.9** Calculating with matrices

Let $k, l, m, n \in \mathbb{N}$, $A, A' \in \text{Mat}(n \times m; F)$, $B, B' \in \text{Mat}(m \times l; F)$, $C \in \text{Mat}(l \times k; F)$ and $I = I_m$. Then the following hold for matrix multiplication

$$\begin{aligned} (A + A')B &= AB + A'B \\ A(B + B') &= AB + AB' \\ IB &= B \\ AI &= A \\ (AB)C &= A(BC) \end{aligned}$$

2.2 Basic properties of matrices

- **Definition 2.2.1** *Invertible*

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

- **Definition 2.2.2** *Elementary matrix*

An *elementary matrix* is any square matrix that differs from the identity matrix in at most one entry.

- **Theorem 2.2.3**

Every square matrix can be written as a product of elementary matrices.

- **Definition 2.2.4** *Smith Normal Form*

Any matrix whose only non-zero entries lie on the diagonal, and which has first 1s on along the diagonal followed by 0s is in *Smith Normal Form*.

- **Theorem 2.2.5** Transformation of a matrix into Smith-Normal form

For each matrix $A \in \text{Mat}(n \times m; F)$ there exist invertible matrices P and Q such that PAQ is a matrix in Smith Normal Form and Q such that PAQ is a matrix in Smith Normal Form.

- **Definition 2.2.6** *Rank*

The *column rank* of a matrix $A \in \text{Mat}(n \times m; F)$ is the dimension of the subspace 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 2.2.7**

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

- **Definition 2.2.8** *Full rank*

Whenever the rank of a matrix is equal to the number of rows (or columns — whichever is smaller), it 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 and W vector spaces over F with ordered bases $\mathcal{A} = (\mathbf{v}_1, \dots, \mathbf{v}_m)$ and $\mathcal{B} = (\mathbf{w}_1, \dots, \mathbf{w}_n)$. Then to each linear mapping $f : V \rightarrow W$ we associated a *representing matrix* ${}_B[f]_A$ whose entries a_{ij} are defined by the identity

$$f(\mathbf{v}_j) = a_{1j}\mathbf{w}_1 + \dots + a_{nj}\mathbf{w}_n \in W$$

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

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

- **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 matrices of f and g

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

- **Definition 2.3.3**

Let V be a finite-dimensional vector spaces with an ordered basis $\mathcal{A} = (\mathbf{v}_1, \dots, \mathbf{v}_m)$. We denote the inverse to the bijection $\Phi_A : F^m \rightarrow V, (\alpha_1, \dots, \alpha_m)^T \mapsto \alpha_1\mathbf{v}_1 + \dots + \alpha_m\mathbf{v}_m$ by

$$\mathbf{v} \mapsto {}_A[\mathbf{v}]$$

The column vector ${}_A[\mathbf{v}]$ is called the *representation of the vector \mathbf{v} with respect to the basis \mathcal{A}* .

- **Theorem 2.3.4** 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 $\mathbf{v} \in V$:

$${}_B[f(\mathbf{v})] = {}_B[f]_A \circ {}_A[\mathbf{v}]$$

2.4 Change of a matrix by change of basis

- **Definition 2.4.1** *Change of basis matrix*

Let $\mathcal{A} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ and $\mathcal{B} = (\mathbf{w}_1, \dots, \mathbf{w}_n)$ be ordered bases of the same F -vector space V . Then the matrix representing the identity mapping with respect to these bases

$${}_B[\text{id}_V]_A$$

is called a *change of basis matrix*. By definition, its entries are given by the equalities $\mathbf{v}_j = \sum_{i=1}^n a_{ij}\mathbf{w}_i$.

- **Theorem 2.4.3** Change of basis

Let V and 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

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

- **Corollary 2.4.4** 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

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

- **Theorem 2.4.5** 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 ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ has zero entries everywhere except possibly on the diagonal, and along the diagonal there are 1s first, followed by 0s.

- **Definition 2.4.6** Trace

The *trace* of a square matrix is defined to be the sum of its diagonal entries. We denote this by

$$\text{tr}(A)$$

3 Rings and Modules

3.1 Rings

- **Group Axioms**

1. Closure
2. Associativity
3. Existence of identity
4. Existence of inverses

- **Definition 3.3.1** Ring

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

1. $(R, +)$ is an abelian group;
2. (R, \cdot) is a *monoid*; this means that the second operation $\cdot : R \cdot R \rightarrow R$ is associative and that there is an *identity element* $1 = 1_R \in R$.
3. The distributive laws hold.

The two operations are called *addition* and *multiplication* in our ring.

A ring in which multiplication is commutative is a *commutative ring*.

- **Proposition 3.1.7** Divisibility by sum

A natural number is divisible by 3 (respectively 9) precisely when the sum of its digits is divisible by 3 (respectively 9).

- **Definition 3.1.8** Field

A *field* F is a non-zero commutative ring in which every non-zero element $a \in F$ has an inverse $a^{-1} \in F$.

- **Proposition 3.1.11**

Let $m \in \mathbb{Z}^+$. The commutative ring $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime.

3.2 Properties of rings

- **Lemme 3.2.1** Additive inverses

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 3.2.3**

Let $m \in \mathbb{Z}$. The m -th multiple ma of an element a in abelian group R is

$$ma = \underbrace{a + a + \cdots + a}_{m \text{ terms}} \quad \text{if } m > 0$$

$0a = 0$, and negative multiples are defined by $(-m)a = -(ma)$.

- **Lemma 3.2.4** Rules for multiples

Let R be a ring, let $a, b \in R$ and let $m, n \in \mathbb{Z}$. 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 3.2.6** Unit

Let R be a ring. An element $a \in R$ is called a *unit* if it is invertible in R or (in other words) has a multiplicative inverse in R .

- **Proposition 3.2.10**

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

- **Definition 3.2.13** Integral domains

An *integral domain* is a non-zero commutative ring that has no zero-divisors.

- **Proposition 3.2.16** Cancellation law for integral domains

Let R be an integral domain and let $a, b, c \in R$.

$$ab = ac \text{ and } a \neq 0 \implies b = c$$

- **Proposition 3.2.17**

Let $m \in \mathbb{N}$. Then $\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if m is prime.

- **Theorem 3.2.18**

Every *finite* integral domain is a field.

3.3 Polynomials

- **Definition 3.1.1**

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

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

for some $m \in \mathbb{N}$ and elements $a_i \in R$ for $i \in [0, m]$.

The set of all polynomials over R is denoted by $R[X]$.

In case a_m is non-zero, the polynomial P has *degree m* , written $\deg(P)$, and a_m is its *leading coefficient*.

When the leading coefficient is 1, the polynomial is a *monic polynomial*.

A polynomial of degree one is called *linear*, a polynomial of degree two is called *quadratic*, and a polynomial of degree three is called *cubic*.

- **Definition 3.3.2** Ring of polynomials

The set $R[X]$ is a ring called the *ring of polynomials over R* . The zero and the identity of $R[X]$ are the zero and identity of R , respectively.

- **Lemma 3.3.3**

1. If R is ring with no zero-divisors, then $R[X]$ has no zero-divisors and $\deg(PQ) = \deg(P) + \deg(Q)$ for non-zero $P, Q \in R[X]$.

2. If R is an integral domain, then so is $R[X]$

• **Theorem 3.3.4** Division and remainder

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

• **Definition 3.3.6**

Let R be a commutative ring and $P \in R[X]$ a polynomial. Then the polynomial P can be *evaluated* at $\lambda \in R$ to produce $P(\lambda)$ by replacing the powers of X in the polynomial P by the corresponding powers of λ . This gives a mapping

$$R[X] \rightarrow \text{Maps}(R, R)$$

An element $\lambda \in R$ is a *root* of P if $P(\lambda) = 0$.

• **Proposition 3.3.9**

Let R be a commutative ring, let $\lambda \in R$ and $P(X) \in R[X]$. Then λ is a root of $P(X)$ if and only if $(X - \lambda)$ divides $P(X)$.

• **Theorem 3.3.10**

Let R a ring, 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 3.3.11** *Algebraically closed*

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

• **Theorem 3.3.13** *Fundamental theorem of algebra*

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

$$P = c(X - \lambda_1) \cdots (X - \lambda_n)$$

with $n \geq 0, c \in F^\times$ and $\lambda_1, \dots, \lambda_n \in F$. This decomposition is unique up to reordering of the factors.

3.4 Homomorphisms, Ideals, and Subrings

• **Definition 3.4.1** *Ring homomorphism*

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

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

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

• **Prelude to ideals**

Let $f : R \rightarrow S$ be a ring homomorphism with $\ker f = \{r \in R : f(r) = 0_S\}$. Then $\ker f$ is:

- a subgroup of R under addition
- $0_R \in \ker f$
- closed under multiplication
- closed under left and right multiplication by arbitrary elements of R
i.e. $x \in \ker f \implies rx, xr \in \ker f \forall r \in R$

• **Lemma 3.4.5**

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

1. $f(0_R) = 0_S$
2. $f(-x) = -f(x)$
3. $f(x - y) = f(x) - f(y)$
4. $f(m \cdot x) = m \cdot f(x)$

Where mx denotes the m -th multiple of x .

• **Definition 3.4.7** *Ideal*

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 (it's a subgroup)
3. $\forall i \in I$ and $\forall r \in R$ we have $ri, ir \in I$ (I is closed under multiplication by elements of R)

Ideals satisfy the properties of rings, except possibly the existence of a multiplicative identity.

Ideals are subrings which are closed under multiplication with elements from the *ring* — not just elements from within the ideal!

• **Definition 3.4.11** *Generated ideal*

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

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

together with the zero element in the case $T = \emptyset$.

• **Proposition 3.4.14**

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 3.4.15** *Principle ideal*

Let R be a commutative ring. An ideal $I \trianglelefteq R$ is called a *principle ideal* if $I = \langle t \rangle$ for some $t \in R$.

• **Definition 3.4.17** *Kernel*

Let R and S be rings, and let $f : R \rightarrow S$ be a ring homomorphism. Since f is in particular a group homomorphism from $(R, +)$ to $(S, +)$, the *kernel* of f already has a meaning:

$$\ker f = \{r \in R : f(r) = 0_S\}$$

• **Proposition 3.4.18**

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

• **Lemma 3.4.20** f is injective if and only if $\ker f = \{0\}$

• **Lemma 3.4.21** The intersection of any collection of ideals of a ring R is an ideal of R .

• **Lemma 3.4.22** Let I and J be ideals of a ring R . Then

$$I + J = \{a + b : a \in I, b \in J\}$$

is an ideal of R .

• **Definition 3.4.23** *Subring*

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

• **Proposition 3.4.26** Test for a subring

Let R be a ring, and $R' \subseteq R$. Then R' is a subring if and only if

1. R' has a multiplicative identity, and
2. R' is closed under subtraction, and
3. R' is closed under multiplication.

• **Proposition 3.4.29** Let R and S be rings 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, 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** *Relation*

A *relation* R on a set X is a subset $R \subseteq X \times X$. R is an *equivalence relation* on X when $\forall x, y, z \in X$ the following hold:

1. *Reflexivity*: xRx
2. *Symmetry*: $xRy \iff yRx$
3. *Transitivity*: xRy and $yRz \implies xRz$

• **Definition 3.5.3**

Suppose that \sim is an equivalence relation on a set X . For $x \in X$ the set $E(x) \equiv \{z \in X : z \sim x\}$ is called the *equivalence class* of x .

A subset $E \subseteq X$ is called an *equivalence class* for \sim if $\exists x \in X \ni E = E(x)$.

An element of an equivalence class is called a *representative* of the class.

A subset $Z \subseteq X$ containing precisely one element from each equivalence class is called a *system of representatives* for the equivalence relation.

• **Definition 3.5.5** *Set of equivalence classes*

Given an equivalence relation \sim on the set X , the *set of equivalence classes*, which is a subset of $\mathcal{P}(X)$, is

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

There is a canonical mapping $\text{can} : X \rightarrow (X/\sim)$, $x \mapsto E(x)$. It is obviously a surjection.

• **Remark**

Suppose that \sim is an equivalence relation on X . If $f : X \rightarrow Z$ is a mapping with the property that $x \sim y \implies f(x) = f(y)$, then there is a unique mapping $\bar{f} : (X/\sim) \rightarrow Z$ with $f = \bar{f} \circ \text{can}$. Its definition is easy: $f(E(x)) = f(x)$. This property is called the *universal property of the set of equivalence classes*.

• **Definition 3.5.7** *Well-defined*

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

3.6 Factor Rings and the First Isomorphic Theorem

• **Prelude**

Let $f : R \rightarrow S$ be a ring homomorphism.

$$x \sim y \iff f(x) = f(y) \iff f(x - y) = 0 \iff x - y \in \ker f$$

Then:

$$E(x) = x + \ker f \equiv \{x + k : k \in \ker f\}$$

So we have that:

- the rule $x \sim y \iff x - y \in \ker f$ is an equivalence relation;
- the equivalence classes are the sets $x + \ker f$ for $x \in R$;
- the set of equivalence classes (R / \sim) is a ring, isomorphic to a subring of S .

• **Definition 3.6.1** *Cosets*

Let $I \trianglelefteq R$ be an ideal in a ring R . The set

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

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

• **Definition 3.6.3** *Factor ring*

Let R be a ring, $I \trianglelefteq R$ be an ideal, and \sim the equivalence relation defined by $x \sim y \iff x - y \in I$. 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 .

$$R/I = \{r + I : r \in R\}$$

• **Theorem 3.6.4**

Let R be a ring, and $I \trianglelefteq R$ an 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

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

• **Theorem 3.6.7** *Universal Property of Factor Rings*

Let R be a ring, and $I \trianglelefteq R$.

1. The mapping $\text{can} : R \rightarrow R/I$ with $\text{can}(r) = r + I$ is a surjective ring homomorphism with kernel I .
2. 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 3.6.9** *First Isomorphic 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

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

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

such that $\forall r, s \in R$ and $a, b \in M$ the following identities hold:

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

i.e. a vector space, but with a *ring* instead of a *field*.

- **Lemma 3.7.8** 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. $(-r)a = r(-a) = -(ra), \quad \forall r \in R, a \in M.$ (Here, the first negative is in R , and the last two negatives are in M .)

- **Definition 3.7.11**

Let R be a ring, and let M, N be R -modules. A mapping $f : M \rightarrow N$ is an R -homomorphism if the following hold $\forall a, b \in M$ 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 $\operatorname{im} f = \{f(a) : a \in M\} \subseteq N$.

If f is a bijection then it is an *isomorphism*.

- **Definition 3.7.15**

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 3.7.20** Test for a submodule

Let R be a ring and let M be an R -module. A subset $M' \subseteq M$ is a submodule if and only if

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

- **Lemma 3.7.21**

Let $f : M \rightarrow N$ be an R -homomorphism. Then $\ker f$ is a submodule of M and $\operatorname{im} f$ is a submodule of N .

- **Lemma 3.7.22**

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

- **Definition 3.7.23**

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

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

together with the zero element in case $T = \emptyset$.

The module M is *finitely generated* if it is generated by a finite set: $M = {}_R\langle \{t_1, \dots, t_n\} \rangle$.

It is *cyclic* if it is generated by a singleton: $M = {}_R\langle t \rangle$.

- **Lemma 3.7.28** Let $T \subseteq M$. Then ${}_R\langle T \rangle$ is the smallest submodule of M that contains T .

- **Lemma 3.7.29** The intersection of any collection of submodules of M is a submodule of M .

- **Lemma 3.7.30** Let M_1 and 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 3.7.31.1 Coset**

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

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

It is a coset of N in the abelian group M and is an equivalence class for the equivalence relation $a \sim b \iff a - b \in N$.

• **Definition 3.7.31.2** *Factor*

M/N , the *factor of M by N* or the *quotient of M by N* , is the set (M / \sim) of all cosets of N in M .

$$M/N = \{a + N : a \in M\}$$

This becomes an R -module by introducing the operations of addition and multiplication as follows:

$$\begin{aligned}(a + N) + (b + N) &= (a + b) + N \\ r(a + N) &= ra + N\end{aligned}$$

for all $a, b \in M, r \in R$.

• **Theorem 3.7.31.3** *Factor module*

- The zero of M/N is the coset $0_{M/N} = 0_M + N$.
- The negative of $a + N \in M/N$ is the coset $-(a + N) = (-a) + N$.
- The R -module M/N is the *factor module* of M by the submodule N .

• **Theorem 3.7.32** The Universal Property of Factor Modules

Let R be a ring, and let L and M be R -modules, and N a sub-module of M .

1. The mapping $\text{can} : M \rightarrow M/N$ sending a to $a + N$, $\forall a \in M$ is a surjective R -homomorphism with kernel 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 3.7.33** First Isomorphism Theorem for Modules

Let R be a ring and let M and N be R -modules. Then every R -homomorphism $f : M \rightarrow N$ induces a R -isomorphism

$$\bar{f} : M / \ker f \rightarrow \text{im } f$$

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 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 σ is called the *length of σ* and written $\ell(\sigma)$. In formulas:

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

The *sign of σ* is defined to be the parity of the number of inversions of σ . In formulas:

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

- **Lemma 4.1.5** (Multiplicativity 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 4.1.7** *Alternating group*

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 .

5 Reference

5.1 Terminology of Algebraic Structures

	<i>Associativity</i>	<i>Identity</i>	<i>Inverses</i>
Group	Yes	Yes	Yes
Monoid	Yes	Yes	No
Semigroup	Yes	No	No
Magma	No	No	No

Ring = (Group, Monoid)

Field = (Group, Group)