# Honours Algebra Notes

Anthony Catterwell

March 5, 2019

## Contents

# 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

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

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

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

  The neutral elements are called $0_F, 1_F$. In particular

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

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

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

  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

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

  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 subspace 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 $\alpha_1, \ldots, \alpha_r \in F$ and $\mathbf{v}_1, \ldots, \mathbf{v}_r \in T$, 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 $\mathcal{U}$:

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

  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 $\mathbf{v}_1, \ldots, \mathbf{v}_r \in L$ and arbitrary vectors $\alpha_1, \ldots, \mathbf{v}_r \in F$,

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

- **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 $\mathbf{v}_1, \ldots, \mathbf{v}_r \in V$ vectors. The family $(\mathbf{v}_i)_{1 \leq i \leq r}$ is a basis of $V$ if and only if the following "evaluation" mapping

$$\Phi : F^r \to V$$
$$(\alpha_1, \ldots, \alpha_r) \mapsto \alpha \mathbf{v}_1 + \cdots + \alpha_r \mathbf{v}_r$$

  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 $f : X \to F$ 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, $L \subset V$ and finite linearly independent subset, and $E \subseteq V$ and generating set. Then there is an injection $\Phi : L \to E$ such that $(E \setminus \Phi(L)) \cup L$ is also a generating set for $V$.
- **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 $f : V \to W$ is called *linear* if for all $\mathbf{v}_1, \mathbf{v}_2 \in V$ and $\lambda \in F$ we have
  $$f(\mathbf{v}_1 + \mathbf{v}_2) = f(\mathbf{v}_1) + f(\mathbf{v}_2)$$
  $$f(\lambda \mathbf{v}_1) = \lambda f(\mathbf{v}_1)$$
  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 $f : X \to X$, we denote the set of fixed points by
  $$X^f = \{x \in X : f(x) = x\}$$
- **Definition 1.7.6:** *Complementary*
  Two vector subspace $V_1, V_2$ of a vector space $V$ are *complementary* if addition defines a bijection
  $$V_1 \times V_2 \to V$$
- **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

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

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

### 1.8 Rank-Nullity theorem

- **Definition 1.8.1:**
  The *image* of a linear mapping $f : V \to W$ is the subset $\mathrm{im}(f) = f(V) \subseteq W$. It is a vector subspace of $W$. The pre-image of the zero vector of a linear mapping $f : V \to W$ 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 $f : V \to W$ is injective if and only if $\ker_f = 0$.

- **Theorem 1.8.4:** Rank-Nullity theorem
  Let $f : V \to W$ be a linear mapping between vector spaces. Then

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

- **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 $F^m \to F^n$ and matrices

- **Theorem 2.1.1:** Linear mappings $F^m \to F^n$ and matrices
  Let $F$ be a field and let $m, n \in \mathbb{N}$. There is a bijection between the space of linear mappings $F^m \to F^n$ and the set of matrices with $n$ rows and $m$ columns and entries in $F$

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

  This attaches to each linear mapping $f$ its *representing matrix* $\mathrm{M}(f) \equiv [f]$. 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 $A \in \mathrm{Mat}(n \times m; F)$ 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
  $$(AB)_{ik} = \sum_{j=1}^{m} A_{ij} B_{jk}$$
  Matrix multiplication produces a mapping
  $$\begin{aligned} \mathrm{Mat}(n \times m; F) \times \mathrm{Mat}(m \times l; F) &\to \mathrm{Mat}(m \times l; F) \\ (A, B) &\mapsto AB \end{aligned}$$

- **Theorem 2.1.8:** Composition of linear mappings and products of matrices
  Let $g : F^l \to F^m$ and $f : F^m \to F^n$ 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 $k, l, m, n \in \mathbb{N}, A, A' \in \mathrm{Mat}(n \times m; F), B, B' \in \mathrm{Mat}(m \times l; F), C \in \mathrm{Mat}(l \times k; F)$ 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 $A \in \mathrm{Mat}(n \times m; F)$ 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 $A \in \mathrm{Mat}(n \times m; F)$ 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 $f : V \to W$ we associated a *representing matrix* ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ 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

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

- **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 matrix of the composition $g \circ f : U \to W$ is the matrix product of the representing matrices of $f$ and $g$

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

- **Definition 2.3.3:**
  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 $\Phi_{\mathcal{A}} : F^m \to V, (\alpha_1, \dots, \alpha_m)^T \mapsto \alpha_1\mathbf{v}_1 + \dots + \alpha_m\mathbf{v}m$ by

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

  The column vector ${}_{\mathcal{A}}[\mathbf{v}]$ is called the *representation of the vector $\boldsymbol{v}$ 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 $f : V \to W$ be a linear mapping. The following holds for $\mathbf{v} \in V$:

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

## 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

$${}_{\mathcal{B}}[\mathrm{id}_V]_{\mathcal{A}}$$

  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 $f : V \to W$ 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

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

- **Corollary 2.4.4:** 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 of $V$. Then

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

- **Theorem 2.4.5:** Smith Normal Form
  Let $f : V \to W$ be a linear mapping between finite-dimensional $F$-vector spaces. There exist an ordered basis $\mathcal{A}$ of $V$ and an ordered basis $\mathcal{B}$W 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

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

# 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 $(R, +, .)$ that satisfy
  1. $(R, +)$ is an abelian group;
  2. $(R, \cdot)$ is a *monoid*; this means that the second operation $\cdot : R \cdot R \to R$ 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

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

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 $\lambda$. This gives a mapping
  $$R[X] \to \text{Maps}(R, R)$$
  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 $\lambda$ 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 an 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 $F$ 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 $\lambda_1, \ldots, \lambda_n \in F$. 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 $f : R \to S$ 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 $f : R \to S$ 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 $f : R \to S$ 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

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

  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 $f : R \to S$ 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 $f : R \to S$ 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 $f : R \to S$ 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 is 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 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 can : $X \to (X/\sim),\ x \mapsto E(x)$. It is obviously a surjection.
- **Remark**
  Suppose that $\sim$ is an equivalence relation on $X$. If $f : X \to Z$ is a mapping with the property that $x \sim y \implies f(x) = f(y)$, then there is a unique mapping $\overline{f} : (X \setminus \sim) \to Z$ with $f = \overline{f} \circ \text{can}$. 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*
  $g : (X/\sim) \to Z$ is *well-defined* if there is a mapping $f : X \to Z$ such that $f$ has the property $x \sim y \implies f(x) = f(y)$ and $g = \overline{f}$.

## 3.6 Factor Rings and the First Isomorphic Theorem

- **Prelude**
  Let $f : R \to S$ 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

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

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 $\text{can} : R \to R/I$ with $\text{can}(r) = r + I$ is a surjective ring homomorphism with kernel $I$.
2. If $f : R \to S$ is a ring homomorphism with $f(I) = \{0_S\}$, so that $I \subseteq \ker f$, then there is a unique ring homomorphism $\overline{f} : R/I \to S$ such that $f = \overline{f} \circ \text{can}$.

- **Theorem 3.6.9:** First Isomorphic Theorem for Rings
Let $R$ and $S$ be rings. Then every ring homomorphism $f : R \to S$ induces a ring isomorphism

$$\overline{f} : R/\ker f \tilde{\to} \text{im} f$$

## 3.7 Modules

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

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

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

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

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. $0_R a = 0_M \ \forall a \in M$
  2. $r0_M = 0_M \ \forall r \in R$
  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 $f : M \to N$ is an *$R$-homomorphism* if the following hold $\forall a, b \in M$ and $r \in R$:
  $$f(a+b) = f(a) + f(b)$$
  $$f(ra) = rf(a)$$
  The *kernel* of $f$ is $\ker f = \{a \in M : f(a) = 0_N\} \subseteq M$ 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 *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 $f : M \to N$ be an $R$-homomorphism. Then $\ker f$ is a submodule of $M$ and $\mathrm{im} f$ is a submodule of $N$.

- **Lemma 3.7.22:**
  Let $R$ be a ring, let $M$ and $N$ be $R$-modules and let $f : M \to N$ 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
  $${}_R\langle T \rangle = \{r_1 t_1 + \cdots + r_m t_m : t_1, \ldots, t_m \in T, r_1, \ldots, r_m \in R\},$$
  together with the zero element in case $T = \emptyset$.
  The module $M$ is *finitely generated* if it is generated by a finite set: $M =_r \langle \{t_1, \ldots, t_n\}$.
  It is *cyclic* f 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 $M$.

- **Theorem-Definition 3.7.31:**
  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 os is an equivalence class for the equivalence relation $a \sim b \iff a - b \in N$.

- **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 submodule of $M$.
  1. The mapping $\text{can} : M \to M/N$ sending $a$ to $a+N$, $\forall a \in M$ is a surjective $R$-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 $\overline{f} : M/N \to L$ such that $f = \overline{f} \circ \text{can}$.
- **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 $f : M \to N$ induces a $R$-isomorphism
  $$\overline{f} : M/\ker f \to \text{im} f$$

# 4 Determinants and Eigenvalues Redux

# 5 Reference

## 5.1 Terminology of Algebraic Structures

| | *Associativity* | *Identity* | *Inverses* |
|---|---|---|---|
| Group | Yes | Yes | Yes |
| Monoid | Yes | Yes | No |
| Semigroup | Yes | No | No |
| Magma | No | No | No |

Ring = (Group, Monoid)

Field = (Group, Group)