1 Vector Spaces

1.1 Fields and Vector Spaces

Definition 1.1.1: Definition of a field

A field F is a set with two functions

- Addition: $+ : F \times F \to F$, $(\lambda, \mu) \mapsto \lambda + \mu$
- Multiplication: $\cdot : F \times F$, $(\lambda, \mu) \mapsto \lambda\mu$

which satisfy the following axioms:

1. $(F, +)$ is an abelian group F^+, with identity 0_F
2. $(F \backslash \{0_F\}, \cdot)$ is an abelian group $F^\times$, with identity 1_F
3. **Distributive law**: For all a, b, and c in F, we have
$$a(b+c) = ab + ac \in F$$

and the following lemmas:

1. The elements 0_F and 1_F of F are distinct
2. For all $a \in F$, $a \cdot 0_F = 0_F$ and $0_F \cdot a = 0_F$
3. Multiplication in F is associative, and 1_F is an identity element

---

A **vector space** V **over a field** F is a pair consisting of an abelian group $V = (V, \dot{+})$ and a mapping
$$F \times V \to V : (\lambda, \vec{v}) \mapsto \lambda\vec{v}$$
s.t. for all $\lambda, \mu \in F$ and $\vec{v}, \vec{w} \in V$ the following identities hold:

- **Distributivity 1**: $\lambda(\vec{v} \dot{+} \vec{w}) = \lambda\vec{v} \dot{+} \lambda\vec{w}$
- **Distributivity 2**: $(\lambda + \mu)\vec{v} = \lambda\vec{v} \dot{+} \mu\vec{v}$
- **Associativity**: $\lambda(\mu\vec{v}) = (\lambda\mu)\vec{v}$
- **Identity**: $1\vec{v} = \vec{v}$

and so do the following lemmas:

1. If V is a vector space and $\vec{v} \in V$, then $0\vec{v} = \vec{0}$
2. If V is a vector space and $\vec{v} \in V$, then $(-1)\vec{v} = -\vec{v}$
3. If V is a vector space over a field F, then $\lambda\vec{0} = \vec{0}$ for all $\lambda \in F$. Furthermore, if $\lambda\vec{v} = \vec{0}$ then either $\lambda = 0$ or $\vec{v} = \vec{0}$

1.2 Working with Vector Spaces

Definition 1.2.1: Cartesian Product of n sets

$$X_1 \times \cdots \times X_n := \{(x_1, \ldots, x_n) : x_i \in X_i \text{ for } 1 \leq i \leq n\}$$
The elements of a product are called **n-tuples**. An individual entry $x_i = (x_1, \ldots, x_n)$ is called a **component**.
There are special mappings called **projections** for a cartesian product:
$$\mathrm{pr}_i : X_1 \times \cdots \times X_n \to X_i$$
$$(x_1, \ldots, x_n) \mapsto x_i$$
The cartesian product of n copies of a set X is written in short as: X^n

Definition 1.2.2: Vector Subspace

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

Definition 1.2.3: Spans and Linear Independence

Let $T \subset V$ for some vector space V over a field F. Then amongus all subspaces of V that include T there is a smallest subspace
$$\langle T \rangle = \langle T \rangle_F \subseteq V$$
"the set of all vectors $\alpha_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r$ with $\alpha_1, \ldots, \alpha_r \in F$ and $\vec{v}_1, \ldots, \vec{v}_r \in T$, together with the zero vector in the case $T = \emptyset$"

Terminology Dump

- An expression of the form $\alpha_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r$ is called a **linear combination** of vectors $\vec{v}_1, \ldots, \vec{v}_r$
- The smallest vector subspace $\langle T \rangle \subseteq V$ containing T is called the **vector subspace generated by** T or the vector subspace **spanned by** T or even the **span of** T
- If we allow the zero vector to be the "empty linear combination of $r = 0$ vectors", then the span of T is exactly the set of all linear combinations of vectors from T
- A subset of a vector space that spans the entire space is called a **generating** or **spanning set**. A vector space that has a finite generating set is said to be **finitely generated**

Linear Independence

A subset L of a vector space V is called **linearly independent** if for all pairwise different vectors $\vec{v}_1, \ldots, \vec{v}_r \in L$ and arbitrary scalars $\alpha, \ldots, \alpha_r \in F$,
$$a_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r = \vec{0} \implies a_1 = \cdots = \alpha_r = 0$$
A subset L of a vector space V is called **linearly dependent** if it is not linearly independent (duh..). This means there exists pairwise different vectors $\vec{v}j_1, \ldots, \vec{v}_r \in L$ and scalars $\alpha_1, \ldots, \alpha_r \in F$, not all zero, such that $\alpha_1\vec{v}_1 + \cdots \alpha_r\vec{v}_r = \vec{0}$

1.3 Linear Independence and Bases

Definition 1.3.1: Basis of a Vector Space

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

Example 1.3.2: Standard Basis

Let F be a field and $n \in \mathbb{N}$. We consider the following vectors in F^n
$$\vec{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$$
with one 1 in the i-th place and zero everywhere else. Then $\vec{e}_1, \ldots, \vec{e}_n$ form an ordered basis of F^n, the so-called **standard basis of** F^n

Theorem 1.3.3: Linear combinations of basis elements

Let F be a field, V a vector space over F and $\vec{v}_1, \ldots, \vec{v}_r \in V$ vectors. The family $(\vec{v}_i)_{1 \leq i \leq r}$ is a basis of V if and only if the following "evaluation" mapping
$$\psi : F^r \to V$$
$$(\alpha_1, \ldots, a_r) \mapsto a_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r$$
is a bijection
If we label our ordered family by $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_r)$, then we done the above mapping by
$$\psi = \psi_{\mathcal{A}} : F^r \to V$$

Theorem 1.3.4: Characterisations 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 $E \backslash \{\vec{v}\}$ does not generate V, for any $\vec{v} \in E$
3. E is maximal among all linearly independent subsets, meaning that $E \cup \{\vec{v}\}$ is linearly dependent for any $\vec{v} \in V$

Corrollary: Let V be a finitely generated vector space over a field F. Then V has a finite basis

---

Basis Characterisation Variant

1. If $L \subset V$ is a linearly independent subset and E is minimal amongst all generating sets of V 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 sets of V with the property $L \subseteq E$, then L is a basis.

Definition 1.3.5: Free Vector Space

Let X be a set and F a field. The set $\mathrm{Maps}(X, F)$ of all mappings $f : X \to F$ becomes an F-vector space with the operations of pointwise addition and multiplication by a scalar. The subset of all mappings which send almost all elements of X to zero is a vector subspace
$$F\langle X \rangle \subseteq \mathrm{Maps}(X, F)$$
This subspace is called the **free vector space on the set** X

Theorem 1.3.6: Variant of Linear Combinations

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

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

1.4 Dimension of a Vector Space

Theorem 1.4.1: Fundamental Estimate of LinAlg

No linearly independent subset of a given vector 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 1.4.2: Steinitz Exchange Theorem

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

Let V be a vector space, $M \subseteq V$ a linearly independent subset, and $E \subseteq V$ a generating subset, such that $M \subseteq E$. If $\vec{w} \in V \backslash M$ is a vector $\notin M$ such that $M \cup \{\vec{w}\}$ is linearly independent, then there exists $\vec{e} \in E \backslash M$ such that $(E \backslash \{\vec{e}\}) \cup \{\vec{w}\}$ is a generating set

Theorem 1.4.3: 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 1.4.4: Dimension of a Vector Space

The cardinality of a basis of a finitely generated vector space V is called the **dimension** of V, written $\dim V$. If F is a field, and we want to denote that we mean dimension as an F-vector space, then we write $\dim_F V$. If the vector space is not finitely generated, then we say $\dim V = \infty$ and call V **infinite dimensional**.

Theorem 1.4.5: Dimension Theorems

Cardinality Criterion for Bases

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

Dimension Estimate for Vector Subspaces: A proper vector subspace of a finite dimensional vector space has itself a strictly smaller dimension

---

If $U \subseteq V$ is a vector subspace of an arbitrary vector space, then we have $\dim U \leq \dim V$ and if we have $\dim U = \dim V < \infty$ then it follows that $U = V$

1.5 Linear Mappings

Definition 1.5.1: Linear Mappings

Let V, W be vector spaces over a field F. A mapping $f : V \to W$ is called **linear**, or F**-linear**, 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

$$f(\vec{v}_1 + \vec{v}_2) = f(\vec{v}_1) + f(\vec{v}_2)$$
$$f(\lambda \vec{v}_1) = \lambda f(\vec{v}_1)$$

A bijective linear mapping is called an **isomorphism** of vector spaces. If there is an isomorphism between two vector spaces, we call them **isomorphic**. A homomorphism $V \to V$ is called an **endomorphism** of V. An isomorphism $V \to V$ is called an **automorphism** of V

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

$$V_1 \times V_2 \xrightarrow{\sim} V$$

something about direct sums

Theorem 1.5.2: Classifying VecSpaces by Dimension

Let n be a natural number. Then a vector space over a field F is isomorphic to F^n iff it has dimension n

Theorem 1.5.3: Linear Mapping and Bases

Let V, W be vector spaces over a field F. The set of all homomorphisms from V to W is denoted by

$$\mathrm{Hom}_F(V, W) = \mathrm{Hom}(V, W) \subseteq \mathrm{Maps}(V, W)$$

Let $B \subset V$ be a basis. Then restriction of a mapping gives a bijection

$$\mathrm{Hom}_F(V, W) \xrightarrow{\sim} \mathrm{Maps}(B, W)$$
$$f \mapsto f|_B$$

Theorem 1.5.4: Inverse Mappings

1. Every injective linear mapping $f : V \hookrightarrow W$ has a **left inverse**, or a linear mapping $g : W \to V$ s.t. $g \circ f = \mathrm{id}_V$
2. Every surjective linear mapping $f : V \twoheadrightarrow W$ has a **right inverse**, or a linear mapping $G : W \to V$ s.t. $f \circ g = \mathrm{id}_W$

Definition 1.5.5: Image and Kernel of a map

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 preimage of the zero vector of a linear mapping $f : V \to W$ is denoted by:

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

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

Mini lemma: A linear mapping is injective iff its kernel is zero

Theorem 1.5.6: Rank-Nullity / Dimension Theorem

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

$$\dim V = \dim(\ker f) + \dim(\mathrm{im}\, f)$$

Dimension of $\mathrm{im}\, f$= **rank** of f, dimension of $\ker f$ = **nullity** of f

---

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 Maps $F^m \to F^n$ 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, m columns, and entries in F:

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

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

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

Definition 2.1.2: Matrix Multiplication

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

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

Theorem 2.1.3: Composition of maps to products

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

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

Theorem 2.1.4: Calculating with Matrices

- (A + A')B = AB + A'B
- A(B + B') + AB + AB'
- IB = B
- AI = A
- (AB)C = A(BC)

2.2 Matrix Definitions

Definition 2.2.1: Big def-thm pairs

Def: A matrix A is called **invertible** if there exists matrices B and C such that $BA = I$ and $AC = I$

Thm: Invertible Equivalence

1. There exists a square matrix B such that $BA = I$
2. There exists a square matrix C such that $AC = I$
3. The square matrix A is invertible

Def: An **elementary matrix** is any square matrix that differs from the identity matrix in at least one entry

Thm: Every square matrix with entries in a field can be written as a product of elementary matrices

Def: 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**

Thm: 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

Thm: Let $f : V \to W$ be a linear map between finite dim. F-vector spaces. There exists two ordered bases $\mathcal{A}$ of V, and $\mathcal{B}$ of W s.t. the representing matrix ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ has zero entries everywhere except possibly on the diagonal, and along the diagonal there are 1's first, followed by 0's

Def: 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.

Thm: The column and row rank of any matrix are equal

Def: Since they are both the same, "column" and "row" can be omitted for the **rank of a matrix**, written as $\text{rk}\, A$. If the rank is equal to the no. of rows/columns, then the matrix has **full rank**

Def: The **trace** of a square matrix is defined to be the sum of its diagonal entries, denoted by $\text{tr}(A)$

2.3 Abstract Linear Mappings and Matrices

Theorem 2.3.1: Representing Matrices

Let F be a field, V and W vector spaces over F with ordered bases $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_m)$ and $\mathcal{B} = (\vec{w}_1, \ldots, \vec{w}_n)$. Then to each linear mapping $f : V \to W$ we associate a **representing matrix** ${}_{\mathcal{B}}[f]\mathcal{A}$ whose entries a_{ij} are defined by the identity

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

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

$$M_{\mathcal{B}}^{\mathcal{A}} : \text{Hom}_F(V, W) \xrightarrow{\sim} \text{Mat}(n \times m; F)$$
$$f \mapsto {}_{\mathcal{B}}[f]_{\mathcal{A}}$$

Theorem 2.3.2: Repr. Mat of Compositions

Let F be a field and U, V, W finite dimensional vector spaces over kF 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: Representation of a vector

Let V be a finite dimensional vector space with an ordered basis $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_m)$. We'll denote the inverse to the bijection in 1.3.3 "$\Phi_{\mathcal{A}} : F^m \xrightarrow{\sim} V, (\alpha_1, \ldots, \alpha_m)^T \mapsto \alpha_1\vec{v}_1 + \cdots + \alpha_m\vec{v}_m$" by

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

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

Thm: Representation of the Image of a Vector: Let V, W be finite dim. 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 $\vec{v} \in V$:

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

2.4 Change of a Matrix by Change of Basis

Definition 2.4.1: Change of Basis Matrix

Let $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_n)$ and $\mathcal{B} = (\vec{w}_1, \ldots, \vec{w}_n)$ be ordered basies of the same F-vector space V. Then the matrix representing the identity mapping w.r.t. these bases

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

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 2.4.2: 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

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

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

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

3 Rings and Modules

3.1 Ring basics

Definition 3.1.1: Definition of a Ring

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

1. $(R, +)$ is an abelian group
2. $(R, \cdot)$ is a **monoid**, meaning that it is a set with **Associativity** and **Identity**, or in other words, a monoid is a group without the neccessity of having the **Inverse** axiom
3. The distributive laws hold, meaning that for all $a, b, c \in R$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c))$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

The two operations are called **addition** and **multiplication** in our ring. A ring in which multiplication, that is $a \cdot b = b \cdot a$ for all $a, b \in R$, is a **commutative ring**

Note: We denote the identity of the monoid $(R, \cdot)$ as 1, and the additive identity of $(R, +)$ as 0_R or 0

Note: We define the **null ring** or **zero ring** as a ring where R is a single element set, i.e. $\{0\}$ where $0 + 0 = 0$ and $0 \times 0 = 0$

Example 3.1.2: Modulo Rings

Let $m \in \mathbb{Z}$. Then the set of **integers modulo** m, written

$$\mathbb{Z}/m\mathbb{Z}$$

is a ring. The elements of $\mathbb{Z}/m\mathbb{Z}$ consist of **congruence classes** of integers modulo m - that is, the elements are the subsets T of $\mathbb{Z}$ of the form $T = a + m\mathbb{Z}$ with $a \in \mathbb{Z}$. Think of these as the set of integers that have the same remainder when you divide them by m. I denote the above congruence class by $\overline{a}$. Obviously $\overline{a} = \overline{b}$ is the same as $a - b \in m\mathbb{Z}$, and often I'll write

$$a \equiv b \mod m$$

3.2 Linking Rings to Fields and Further Properties

Definition 3.2.1: Ring definition of a field

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 $a \cdot a^{-1} = a^{-1} \cdot a = 1$

Definition 3.2.2: Multiples of an abelian group

Let $m \in \mathbb{Z}$. The **m-th multiple ma of an element** $a$in an 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 $(-m)a = -(ma)$

Theorem 3.2.3: Properties of Rings

Lemma set 1: 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 set 2: Let R be a ring, $a, b \in R$ 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. $(ma)(nb) = (mn)(ab)$

Prime Property for Fields: Let m be a natural number. The commutative ring $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime

Definition 3.2.4: Unit of a ring

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, meaning that there exists $a^{-1} \in R$ such that

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

Thm: The set $R^\times$ of units in a ring R forms a group under multiplication

Definition 3.2.5: zero-divisors of a ring

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 $ba = 0$.

Definition 3.2.6: Integral Domain

An **integral domain** is a non-zero commutative ring that has no zero-divisors. The following two laws hold:

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

Theorem 3.2.7: Integral Domain Properties

- **Cancellation Law**: Let R be an integral domain and let $a, b, c \in R$. If $ab = ac$ and $a \neq 0$ then $b = c$
- Let m be a natural number. Then $\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if m is prime.
- Every **finite** integral domain is a field.

3.3 Polynomials

Definition 3.3.1: Polynomial

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 non-negative $m \in \mathbb{Z}$ 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 the case where 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**, degree two is called **quadractic**, and degree three is called **cubic**.

Definition 3.3.2: Ring of Polynomials

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, respectively.

Theorem 3.3.3: Properties of a Polynomial Ring

- If R is a ring with no zero-divisors, then $R[X]$ has no zero-divisors and $\deg(PQ) = \deg(P) + \deg(Q)$ for non-zero $P, Q \in R[X]$.
- If R is an integral domain, then so is $R[X]$
- 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 3.3.4: Evaluating a Function

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

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

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

Thm: 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 3.3.5: Degrees of Polynomial Roots

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

Definition 3.3.6: Algebraically closed fields

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

Theorem 3.3.7: The Fundamental Theorem of Algebra

The field of complex numbers $\mathbb{C}$ is algebraically closed.

Theorem 3.3.8: Linear Factors of Closed Fields

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

3.4 Homomorphisms, Ideals, and Substrings

Definition 3.4.1: Ring Homomorphisms

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

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

Theorem 3.4.2: Properties of Ring Homomorphisms

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

1. $f(0_R) = 0_S$, where 0_R and 0_S are the zeros of R and S
2. $f(-x) = -f(x)$
3. $f(x - y) =$ f(x) - f(y)
4. $f(mx) = mf(x)$
5. $f(x^n) = (f(x))^n$ for all $x \in R$ and $n \in \mathbb{N}$

Definition 3.4.3: Ideal

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

1. $I \neq \emptyset$
2. I is closed under subtraction
3. for all $i \in I$ and $r \in R$ we have $ri, ir \in I$

Definition 3.4.4: Generated Ideals

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

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

Theorem 3.4.5

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 3.4.6: Principal Ideal

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

Theorem 3.4.7: Kernels as Ideals

- Let R and S be rings and $f : R \to S$ a ring homomorphism. Then $\ker f$ is an ideal of R.
- f is injective if and only if $\ker f = \{0\}$
- The intersection of any collection of ideals of a ring R is an ideal of R
- 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 3.4.8: Subrings

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

Thm: Test for subring: Let R be a subset of a ring R. Then R' is a subring iff:

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

Thm: 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, $\operatorname{im} f$ 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 $f|_{R^X} : R^X \to S^X$

3.5 Equivalence Relations

Definition 3.5.1: Equivalence Relations

A **relation** R on a set X is a subset $R \subseteq X \times X$. In the context of relations, it's written xRy instead of $(x, y) \in R$. R is an **equivalence relation on** X when for all elements $x, y, z \in X$ the following hold:

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

Definition 3.5.2: Equivalence Classes

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 class is called a **representive** 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 3.5.3: Set of Equivalence Classes

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

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

There is a canonical mapping $\mathrm{can} : X \to (X/\sim)$, $x \mapsto E(x)$ (surjection)

3.6 Factor Rings and First Isomorphism Theorem

Definition 3.6.1: Coset

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

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

is a **coset of** I **in** R or the **coset of** x **w.r.t** I **in** R

Definition 3.6.2: 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

Theorem 3.6.3

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

$$(x + I)\dot{+}(y + I) = (x + y) + I \qquad \text{for all } x, y \in R$$

and multiplication is defined by

$$(x + I) \cdot (y + I) = xy + I \qquad \text{for all } x, y \in R$$

Theorem 3.6.4: Universal Property of Factor Rings

Let R be a ring and I an ideal of R

1. The mapping $\mathrm{can} : R \to R/I$ sending r to $r + I$ for all $r \in R$ 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 $f = \overline{f} \circ \mathrm{can}$

Theorem 3.6.5: First Isomorphism Theorem for Rings

Let R and S be rings. Then every ring homomorphism $f : R \to S$ induces a ring isomorphism

$$\overline{f} : R/\ker f \xrightarrow{\sim} \operatorname{im} f$$

3.7 Modules

Definition 3.7.1: Module

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

$$R \times M \to M$$
$$(r, a) \mapsto ra$$

s.t. for all $r, s \in R$ and $a, b \in M$, we have:

- **Distributivity 1**: $r(a\dot{+}b) = (ra)\dot{+}(rb)$
- **Distributivity 2**: $(r + s)a = (ra)\dot{+}(sa)$
- **Associativity**: $r(sa) = (rs)a$
- **Identity**: $1_Ra = a$

Theorem 3.7.2: Module Lemmas

Let R be a ring and M an R-module

1. $0_Ra = 0_M$ for all $a \in M$
2. $r0_m = 0_M$ for all $r \in R$
3. $(-r)a = r(-a) = -(ra)$ for all $r \in R$, $a \in M$

Definition 3.7.3: Module Homomorphisms

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

$$f(a+b) = f(a) + f(b)$$
$$f(ra) = rf(a)$$

- The **kernel** of f is $\ker f = \{a \in M : f(a) = 0_N\} \subseteq M$
- The **image** of f is $\operatorname{im} f = \{f(a) : a \in M\} \subseteq N$
- If f is a bijection then it is an **R-module isomorphim** or **isomorphism**, written $M \cong N$, and say M and N are **isomorphic**

Definition 3.7.4: Submodules

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'

Thm: Let R be a ring and let M be an R-module. A subset M' of M is a submodule if and only if

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

Theorem 3.7.5: Submodule lemmas

- Let $f : M \to N$ be an R-homomorphism. Then $\ker f$ is a submodule of M and $\operatorname{im} f$ is a submodule of N
- Let R be a ring, M an R-homomorphism. Then f is injective if and only if $\ker f = \{0_M\}$

Definition 3.7.6: Generated Submodules

Let R be a ring, M an R-module nad let $T \subseteq M$. Then the **submodule of M 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 $T = \emptyset$. If $T = \{t_1, \ldots, t_n\}$, a finite set, we write ${}_R\langle t_1, \ldots, t_n\rangle$ instead of ${}_R\langle\{t_1, \ldots, t_n\}\rangle$. The module M is **finitely generated** if it is generated by a finite set: $M = {}_R\langle t_1, \ldots, t_n\rangle$. It is called **cyclic** if it is generated by a singleton $M = {}_R\langle T\rangle$

Definition 3.7.7: Generated Submodule lemmas

- Let $T \subseteq M$. Then ${}_R\langle T\rangle$ is the smallest submodule of M that contains T
- The intersection of any collection of submodules of M is a submodule of M.
- Let M_1 and M_2 be submodules of a M. Then
$$M_1 + M_2 = \{a + b : a \in M_1, b \in M_2\}$$
is a submodule of M

Definition 3.7.8: Submodule Cosets

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 so is an equivalence class for the equivalence relation $a \sim b \iff a - b \in N$.

Let M/N, the **factor of N by N** or the **quotient of M by N** to be the set $(M/\sim)$ of all cosets of N in M. This becomes an R-module by introducing the operations of addition and multiplication as follows:

$$(a+N)\dot{+}(b+N) = (a+b) + N$$
$$r(a+N) = ra + N$$

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

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 3.7.9: Universal Property of Factor Modules

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

1. The mapping $\text{can} : M \to M/N$ sending a to $a + N$ for all $a \in M$ 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 3.7.10: First Isomorphism Thm for Modules

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

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

4 Determinants and Eigenvalues Redux

4.1 Symmetric Groups

Definition 4.1.1: Symmetric Groups

The group of all permutations of the set $\{1, 2, \ldots, n\}$, also known as bijections from $\{1, 2, \ldots, n\}$ to itself is denoted by $\mathfrak{S}_n$ (but i will just write S_n because icba) and called the **n-th symmetric group**. It is a group under composition and has $n!$ elements.

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

Definition 4.1.2: Inversions of a permutation

An **inversion** of a permutation $\sigma \in S_n$ 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:

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

Theorem 4.1.3: Multiplicativity of the sign

For each $n \in \mathbb{N}$ the sign of a permutation produces a group homomorphism $\operatorname{sgn} : S_n \to \{+1, -1\}$ from the symmetric group to the two-element group of signs. In formulas:

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) \quad \forall \sigma, \tau \in S_n$$

Definition 4.1.4: Alternating Group of a Permutation

For $n \in \mathbb{N}$, the set of even permutations in S_n forms a subgroup of S_n because it is the kernel of the group homomorphism $\operatorname{sgn} : S_n \to \{+1, -1\}$. This group is the **alternating group** and is denoted A_n

4.2 Determinants

Definition 4.2.1: Determinants - the Leibniz Formula

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

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \mapsto \det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)}$$

The sum is over all permutations of n, and the coefficient $\operatorname{sgn}(\lambda)$ is the sign of the permutation σ defined above. When $n = 0$, the determinant is 1

4.3 Characterising the Determinant

Definition 4.3.1: Bilinear Forms

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

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

A bilinear form H is **symmetric** is $U = V$ and

$$H(u, v) = H(v, u) \quad \text{for all } u, v \in U$$

while it is **antisymmetric** or **alternating** if $U = V$ and

$$H(u, u) = 0 \quad \text{for all } u \in U$$

- antisymmetric $\implies$ $H(u, v) = -H(v, u)$
- $H(u, v) = -H(v, u) \implies$ antisymmetric iff $1_F + 1_F \neq 0_F$

Definition 4.3.2: Multilinear Forms

Let $V_1, \ldots, V_n, W$ be F-vector spaces. A mapping $H : V_1 \times V_2 \times \cdots \times V_n \to W$ is a **multilinear form** or just **multilinear** if for each j, the mapping $V_j \to W$ defined by $v_j \mapsto H(v_1, \ldots, v_j, \ldots, v_n)$, with the $v_i \in V_i$ arbitrary fixed vectors of V_i for $i \neq j$ is linear.

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

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

Theorem 4.3.3: Characterisation of the Determinant

Let F be a field. The mapping

$$\det : \mathrm{Mat}(n; F) \to F$$

is the unique alternating multilinear form on n-tuples of column vectors with values in F that takes the value 1_F on the identity matrix

4.4 Rules for Calculating with Determinants

Theorem 4.4: Determinant Theorem Bank

4.4.1: Let R be a commutative ring, $A, B \in \mathrm{Mat}(n; R)$. Then

$$\det(AB) = \det(A)\det(B)$$

4.4.2: The determinant of a square matrix with entries in a field F is non-zero if and only if the matrix is invertible

4.4.3:
- If A is invertible then $\det(A^{-1}) = \det(A)^{-1}$
- If B is a square matrix then $\det(A^{-1}BA) = \det(B)$

4.4.4: For all $A \in \mathrm{Mat}(n; R)$ with R a commutative ring,

$$\det(A^T) = \det(A)$$

Definition 4.4.6: Cofactors of a Matrix

Let $A \in \mathrm{Mat}(n; R)$ for some commutative ring R and $n \in \mathbb{N}$. Let $i, j \in \mathbb{Z}$ between 1 and n. Then the (i, j) **cofactor of A** is $C_{ij} = (-1)^{i+j} \det(A\langle i, j\rangle)$ where $A\langle i, j\rangle$ is the matrix obtained from A by deleting the i-th row and j-th column.

$$C_{23} = (-1)^{2+3} \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = -a_{11}a_{32} + a_{31}a_{12}$$

Theorem 4.4.7: Laplace's Expansion

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

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

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

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

Definition 4.4.8: Adjugate Matrix

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

Theorem 4.4.9: Cramer's Rule

Let A be a $(n \times n)$-matrix with entries in a commutative ring R. Then

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

Theorem 4.4.11: Invertibility of Matrices

A square matrix with entries in a commutative ring R is invertible if and only if its determinant is a unit in R. That is, $A \in \mathrm{Mat}(n; R)$ is invertible if and only if $\det(A) \in R^\times$

Theorem 4.4.14: Jacobi's Formula

Let $A = (a_{ij})$ where the coefficients $a_{ij} = a_{ij}(t)$ are functions of t. Then

$$\frac{d}{dt} \det A = \mathrm{TrAdj} A \frac{dA}{dt}$$

4.5 Eigenvalues and Eigenvectors

Definition 4.5.1: Eigenvalues and Eigenvectors

Let $f : V \to V$ be an endomorphism of an F-vector space V. A scalar $\lambda \in F$ is an **eigenvalue of f** if and only if there exists a non-zero vector $\vec{v} \in V$ such that $f(\vec{v}) = \lambda \vec{v}$. Each such vector is called an **eigenvector of f with eigenvalue λ**. For any $\lambda \in F$, the **eigenspace of f with eigenvalue λ** is

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

Theorem 4.5.4: Existence of Eigenvalues

Each endomorphism of a non-zero finite dimensional vector space over an algebraically closed field has an eigenvalue

Definition 4.5.6: Characteristic Polynomial

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

$$\chi_A(x) := \det(xI_n - A)$$

(where χ stands for χaracteristic, lol)

Theorem 4.5.8: EVs and Characteristic Polynomials

Let F be a field and $A \in \mathrm{Mat}(n; F)$ a square matrix with entries in F. The eigenvalues of the linear mapping $A : F^n \to F^n$ are exactly the roots of the characteristic polynomial χ_A

Theorem 4.5.9: Eigenvalue Remarks

- Square matrices $A, B \in \mathrm{Mat}(n; R)$ of same size are **conjugate** if
$$B = P^{-1}AP \in \mathrm{Mat}(n; R)$$
for an invertible $P \in GL(n; R)$
- Conjugacy is an equivalence relation on $\mathrm{Mat}(n; R)$
- The char. polynomials for two conjugate matrices are the same
- We can define the char. polynomials of an endomorphism $f : V \to V$ of an n-dim vector space over a field F to be
$$\chi_f(x) = \chi_{\mathcal{A}}(x) \in F[x]$$
with $A = {}_{\mathcal{A}}[f]_{\mathcal{A}} \in \mathrm{Mat}(n; R)$ the matrix of f w.r.t *any* basis $\mathcal{A}$ for V. The E.V.s of f are exactly the roots of χ_f

Theorem 4.5.10: Extending Bases

Let $f : V \to V$ be an endomorphism of an n-dimensional vector space V over a field F. Suppose given an m-dimensional subspace $W \subseteq V$ such that $f(W) \subseteq W$, so that there are defined endomorphisms of the subspace and the quotient space:
$$g : W \to W;\ \vec{w} \mapsto f(\vec{w})$$
$$h : V/W \to V/W;\ W + \vec{v} \mapsto W + f(\vec{v})$$
The characteristic polynomial of f is the product of the characteristic polynomials of g and h

4.6 Triangularisable, Diagonalisable, and Cayley-Hamilton

Definition 4.6.1: Triangularisability

Let $f : V \to V$ be an endomorphism of a finite dimensional F-vector space V. f is **triangularisable** if the vector space V has an ordered basis $\mathcal{B} = (\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n)$ such that
$$\begin{aligned} f(\vec{v}_1) &= a_{11}\vec{v}_1, \\ f(\vec{v_2}) &= a_{12}\vec{v}_1 + a_{22}\vec{v}_2, \\ &\vdots \\ f(\vec{v}_n) &= a_{1n}\vec{v}_1 + a_{2n}\vec{v}_2 + \cdots + a_{nn}\vec{v}_n \in V \end{aligned}$$
(so that the first basis vector $\vec{v}_1$ is an eigenvector, with eigenvalue a_{11}) or equivalently such that the $n \times n$ matrix ${}_{\mathcal{B}}[f]_{\mathcal{B}} = (a_{ij})$ representing f with respect to $\mathcal{B}$ is upper triangular (or any other triangular)
$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} \end{pmatrix}$$

Theorem 4.6.1 - 4.6.3

Let $f : V \to V$ be an endomorphism of a finite dimensional F-vector space V. Then f is triangularisable iff the characteristic polynomial χ_f decomposes into linear factors in $F[x]$

Finding ordered bases - Choose from the following subspaces

1. $W = \{\mu\vec{v}_1 \mid \mu \in F\} \subseteq V$
2. $W' = \ker(f - \lambda 1_V)$. This has a basis of E.Vs $\{\vec{v}_1, \ldots, \vec{v}_r\}$
3. $W'' = \mathrm{im}(\lambda 1_V - f)$

Then extend the basis to another ordered basis $\mathcal{B}$ for V(the full space) where $\mathrm{can}(\vec{v}_j) = \vec{u}_j$ forms a basis for V/W. ${}_{\mathcal{B}}[f]_{\mathcal{B}}$ is upper triangular.

An endomorphism $A : F^n \to F^n$ is triangularisable iff $A = (a_{ij})$ is conjugate to $B = (b_{ij})(b_{ij} = 0$ for $i > j)$, an upper triangular matrix, with $P^{-1}AP = B$ for an invertible matrix P

Definition 4.6.6: Diagonalisability

An endomorphism $f : V \to V$ of an F-vector space V is **diagonalisable** iff there exists a basis of V consisting of eigenvectors of f. If V is finite dimensional then this is the same as saying that there exists an ordered basis $\mathcal{B} = \{\vec{v}_1, \ldots, \vec{v}_n\}$ where ${}_{\mathcal{B}}[f]_{\mathcal{B}} = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. In this case, of course, $f(\vec{v}_i) = \lambda_i\vec{v}_i$.

A square matrix $A \in \mathrm{Mat}(n; F)$ is **diagonalisable** iff A is conjugate to a diagonal matrix, i.e. there exists $P \in \mathrm{GL}(n; F)$ such that $P^{-1}AP = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. In this case the columns P are the vectors of a basis of F^n consisting of eigenvectors of A with eigenvalues $\lambda_1, \ldots, \lambda_n$

Theorem 4.6.9: Linear Independence of Eigenvectors

Let $f : V \to V$ be an endomorphism of a vector space V and let $\vec{v}_1, \ldots, \vec{v}_n$ be eigenvectors of f with pairwise different eigenvalues $\lambda_1, \ldots, \lambda_n$. Then the vectors $\vec{v}_1, \ldots, \vec{v}_n$ are linearly independent

Theorem 4.6.10: Cayley-Hamilton Theorem

Let $A \in \mathrm{Mat}(n; R)$ be a square matrix with entries in a commutative ring R. Then evaluating its characteristic polynomial $\chi_A(x) \in R[x]$ at the matrix A gives zero.

4.7 Markov Matrices

Definition 4.7.5: Markov Matrix

A matrix M whose entires are non-negative and s.t. the sum of the entries of each column equals 1 is a **Markov matrix** or a **stochastic matrix**

4.7.6: Suppose $M \in \mathrm{Mat}(n; \mathbb{R})$ is a M.M. Then $\lambda = 1$ is an e.v.

Theorem 4.7.10: Perron-Frobenius Theorem

If $M \in \mathrm{Mat}(n; \mathbb{R})$ is a Markov matrix with positive values, then the eigenspace $E(1, M)$ is one-dimensional. There exists a unique basis vector $\vec{v} \in E(1, M)$ with positive real entries s.t. the sum of its entries is 1

5 Inner Product Spaces

5.1 Inner Product Spaces Intro

Definition 5.1.1: Inner Product

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

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

A **real inner product space** is a real vector space equipped with an inner product. **Note**: basically a generalisation of dot prod.

A **complex inner product space** is a complex vector space equipped with an inner product. This is the exact same, but condition 2 uses $(\vec{x}, \vec{y}) = \overline{(\vec{y}, \vec{x})}$ where $\overline{z}$ is the complex conjugate

Definition 5.1.5: Norm

In a real or complex inner product space, the **length** or **inner product norm** or **norm** $\|\vec{v}\| \in \mathbb{R}$ of a vector $\vec{v}$ is defined as the non-negative square root
$$\|\vec{v}\| = \sqrt{(\vec{v}, \vec{v})}$$
Vectors whose length are 1 are called **units**. Two vectors $\vec{v}, \vec{w}$ are **orthogonal**, written $\vec{v} \perp \vec{w}$, iff $(\vec{v}, \vec{w}) = 0$

The norm $\|\cdot\|$ on an inner product spacse V satisfies, for any $\vec{v}, \vec{w} \in V$ and scalar λ:

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

Definition 5.1.7: Orthonormal Family

A family $(\vec{v}_i)_{i\in I}$ for vectors from an inner product space is an **orthonormal family** if all the vectors $\vec{v}_i$ have length 1 and if they are pairwise orthogonal to each other, which, if $\delta_{i,j}$ is the **Kronecker delta** defined by

$$\delta_{i,j} = \begin{cases} 1 & i = j \\ 0 & \text{otherwise} \end{cases}$$

means that $(\vec{v}_i, \vec{v}_j) = \delta_{ij}$.
An orthonormal family that has a basis is an **orthonormal basis**

Thm 5.1.10: Every finite dimensional inner product space has an orthonormal basis

5.2 Orthogonal Complements and Projections

Definition 5.2.1: Orthogonals to a Subset

Let V be an inner product space and let $T \subseteq V$ be an arbitrary subset. Define

$$T^{\perp} = \{\vec{v} \in V : \vec{v} \perp \vec{t}\, \forall \vec{t} \in T\}$$

calling this set the **orthogonal** to T

Theorem 5.2.2: Complementary Othorgonals

Let V be an inner product space and let U be a finite dimensional subspace of V. Then U and $U^{\perp}$ are complementary in the sense of 1.5.1. i.e. $V = U \oplus U^{\perp}$

Definition 5.2.3: Orthogonal Projection

Let U be a finite dimensional subspace of an inner product space V. The space $U^{\perp}$ is the **orthogonal complement to** U. The **orthogonal projection from** V **onto** U is the map

$$\pi_U : V \to V$$

that sends $\vec{v} = \vec{p} + \vec{r}$ to $\vec{p}$

Prop 5.2.4: Let U be a finite dimensional subspace of an inner product space V and let π_U be the orthogonal projection from V onto U

1. π_U is a linear mapping with $\text{im}(\pi_U) = U$ and $\ker(\pi_U) = U^{\perp}$
2. If $\{\vec{v}_1, \dots, \vec{v}_n\}$ is an orthonormal basis of U, then π_U is given by the following formula for all $\vec{v} \in V$
$$\pi_U(\vec{v}) = \sum_{i=1}^{n} (\vec{v}, \vec{v}_i)\vec{v}_i$$
3. $\pi_U^2 = \pi_U$, that is, π_U is an idempotent

Theorem 5.2.5: Cauchy-Shwarz Inequality

Let $\vec{v}$, $\vec{w}$ be vectors in an inner product space. Then

$$|(\vec{v}, \vec{w})| \leq \|\vec{v}\|\|\vec{w}\|$$

with equality if and only if $\vec{v}$ and $\vec{w}$ are linearly dependent

Theorem 5.2.7: Gram-Shmidt Process

Let $\vec{v}_1, \dots, \vec{v}_k$ be linearly independent vectors in an inner product space V. Then there exists an orthonormal family $\vec{w}_1, \dots, \vec{w}_k$ with the property that for all $1 \leq i \leq k$,

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

TODO: write how to actually do the gram-shmidt process

5.3 Adjoints and Self-Adjoints

Definition 5.3.1: Adjoints

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

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

In this case I will write $S = T^*$ and call S the **adjoint** of T

Remark 5.3.2: Any endomorphism has at most one adjoint.

Theorem 5.3.4

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

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

Definition 5.3.5: Self Adjoints

An endomorphism of an inner product space $T : V \to V$ is **self-adjoint** if it equals its own adjoint, i.e. if $T^* = T$

Theorem 5.3.7: Self-Adjoint Theorem bank

Let $T : V \to V$ be a self-adjoint linear mapping on an inner product space V

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

Definition 5.3.11: Orthogonal Matrices

An **Orthogonal matrix** is an $(n \times n)$-matrix P with real entries such that $P^T P = I_n$, or in other words such that $P^{-1} = P^T$

Definition 4.3.14: Complex Matrices

A **hermitian matrix** is one that is self-adjoint in $\mathbb{C}$, or in other words one where $A = \overline{A}^T$ holds
An **unitary matrix** is an $(n \times n)$-matrix P with complex entries such that $\overline{P}^T P = I_n$, or such that $P^{-1} = \overline{P}^T$

Theorem 5.3.9: Spectral Theorems

5.3.9: The Spectral Theorem for Self-Adjoint Endomorphisms
Let V be a finite dimensional inner product space and let $T : V \to V$ be a self-adjoint linear mapping. Then V has an orthonormal basis consisting of eigenvalues of T.

5.3.11: The Spectral Theorem for Real Symmetric Matrices
Let A be a real $(n \times n)$-symmetric matrix. Then there is an $(n \times n)$-orthogonal matrix P such that

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

where $\lambda_1, \dots, \lambda_n$ are the (necessarily real) eigenvalues of A, repeated according to their multiplicity as roots of χ_A

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

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

where $\lambda_1, \dots, \lambda_n$ are the (necessarily real) eigenvalues of A, repeated according to their multiplicity as roots of χ_A

6 Jordan Normal Form

6.1 Motivation

no time for motivation over here

6.2 The Jordan Normal Form

Definition 6.2.1: Jordan Blocks

Given an integer $r \geq 1$ define an $(r \times r)$-matrix $J(r)$ called the **nilpotent Jordan block of size** r, by the rule $J(r)_{ij} = 1$ for $j = i + 1$ AND $J(r)_{ij} = 0$ otherwise
In particular, $J(1)$ is a (1×1)-matrix whose only entry is zero.

Given an integer $r \geq 1$ and a scalar $\lambda \in F$, define an $(r \times r)$-matrix $J(r, \lambda)$ called the **Jordan block of size** r **and eigenvalue** λ by the rule

$$J(r, \lambda) = \lambda I_r + J(r) = D + N$$

with $\lambda I_r = \text{diag}(\lambda, \lambda, \dots, \lambda) = D$ diagonal and $J(r) = N$ nilpotent such that $DN = ND$

Theorem 6.2.2: Jordan Normal Form

Let F be an algebraically closed field. Let V be a finite dimensional vector space and let $\phi : V \to V$ be an endomorphism of V with characteristic polynomial

$$\chi_\phi(x) = (x-\lambda_1)^{a_1}(x-\lambda_2)^{a_2}..(x-\lambda_s)^{a_s} \in F[x], a_i \geq 1, \sum_{i=1}^{s} a_i = n$$

For distinct $\lambda_1, \lambda_2, \ldots, \lambda_s \in F$. Then there exists an ordered basis $\mathcal{B}$ of V such that the matrix of ϕ with respect to the block $\mathcal{B}$ is block diagonal with Jordan blocks on the diagonal, ${}_\mathcal{B}[\phi]_\mathcal{B}$

$$= \operatorname{diag}(J(r_{11}, \lambda_1), \ldots, J(r_{1m_1}, \lambda_1), J(r_{21}, \lambda_2), \ldots, J(r_{sm_s}, \lambda_s))$$

with $r_{11}, \ldots, r_{1m_1}, r_{21,\ldots,r_{sm_s}} \geq 1$ such that

$$a_i = r_{i_1} + r_{i_2} + \cdots + r_{im_i} \quad (1 \leq i \leq s)$$

Theorem 6.3.1: Bézout's identity for polynomials

For a characteristic polynomial

$$\chi_\phi(x) = \prod_{i=1}^{s} (x - \lambda_i)^{a_i} \in F[x]$$

where each a_i is a positive integer, $\lambda_i \neq \lambda_j$ for $i \neq j$, and λ_i are e.v.s of ϕ. For each $1 \leq j \leq s$ define

$$P_j(x) = \prod_{\substack{i=1 \\ i \neq j}}^{s} (x - \lambda_i)^{a_i}$$

There exists polynomials $Q_j(x) \in F[x]$ such that

$$\sum_{j=1}^{s} P_j(x) Q_j(x) = 1$$

Definition 6.3.2: Generalised Eigenspace

The **generalised eigenspace** of ϕ with eigenvalue λ_i, $E^{\text{gen}}(\lambda_i, \phi)$ is the following subspace of V:

$$E^{\text{gen}}(\lambda_i, \phi) = \{\vec{v} \in V \mid (\phi - \lambda_i \operatorname{id}_V)^{a_i}(\vec{v}) = \vec{0}\}$$

The dimension of $E^{\text{gen}}(\lambda_i, \phi)$ is called the **algebraic multiplicity of ϕ with eigenvalue** λ_i while the dimension of the eigenspace $E(\lambda_i, \phi)$ is called the **geometric multiplicity of ϕ with eigenvalue λ**

Remark 6.3.4: The actual eigenspace is defined by

$$E(\lambda_i, \phi) = \{\vec{v} \in V \mid (\phi - \lambda_i \operatorname{id}_V)(\vec{v}) = \vec{0}\}$$

$E^{\text{gen}}(\lambda_i, \phi) \subseteq E^{\text{gen}}(\lambda_i, \phi)$, or the algebraic multiplicity of any e.v. must be greater or equal to the corresponding geometric multiplicity

Definition 6.3.4: Stable subsets

Let $f : X \to X$ be a mapping from a set X to itself. A subset $Y \subseteq X$ is **stable under** f precisely when $f(Y) \subseteq Y$, that is if $y \in Y$ then $f(y) \in Y$.

Theorem 6.3.5: Direct Sum Composition

For each $1 \leq i \leq s$, let

$$\mathcal{B}_i = \{\vec{v}_{ij} \in V \mid 1 \leq j \leq a_i\}$$

be a basis of $E^{\text{gen}}(\lambda_i, \phi)$, where a_i is the algebraic multiplicity of ϕ with eigenvalue λ_i s.t. $\sum_{i=1}^{s} a_i = n$ is the dimension of V.

1. Each $E^{\text{gen}}(\lambda_i, \phi)$ is stable under ϕ
2. For each $\vec{v} \in V$ there exist unique $\vec{v}_i \in E^{\text{gen}}(\lambda_i, \phi)$ such that $\vec{v} = \sum_{i=1}^{s} \vec{v}_i$. In other words, there is a direct sum decomposition

$$V = \bigoplus_{i=1}^{s} E^{\text{gen}}(\lambda_i, \phi)$$

with ϕ restricting to endomorphisms of the summands

$$\phi_i = \phi| : E^{\text{gen}}(\lambda_i, \phi) \to E^{\text{gen}}(\lambda_i, \phi)$$

3. Then

$$\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_s = \{\vec{v}_{ij} \mid 1 \leq i \leq s, 1 \leq j \leq a_i\}$$

is a basis of V. The matrix of the endomorphism ϕ w.r.t. this basis is given by the block diagonal matrix

$${}_\mathcal{B}[\phi]_\mathcal{B} = \left(\begin{array}{c|c|c|c} B_1 & 0 & 0 & 0 \\ \hline 0 & B_2 & 0 & 0 \\ \hline 0 & 0 & \ddots & 0 \\ \hline 0 & 0 & 0 & B_s \end{array}\right) \in \operatorname{Mat}(n; F)$$

with $B_i = {}_{\mathcal{B}_i}[\phi_i]_{\mathcal{B}_i} \in \operatorname{Mat}(a_i; F)$

Theorem 6.3: JNF Theorem Bank

6.3.6: For each i, define a linear mapping

$$\psi_i : \frac{W_i}{W_{i-1}} \to \frac{W_{i-1}}{W_{i-2}}$$

by $\psi_i(\vec{w} + W_{i-1}) = \psi(\vec{w}) + W_{i-2}$ for $\vec{w} \in W_i$. Then ψ_i is well-defined and injective

6.3.7: Let $f : X \to Y$ be an injective linear mapping between the F-vector spaces X and Y. If $\{\vec{x}_1, \ldots, \vec{x}_t\}$ is a linearly independent set in X, then $\{f(\vec{x}_1, \ldots, \vec{x}_t)\}$ is a linearly independent set in Y

6.3.8: The set of elements $\{\vec{v}_{j,k} : 1 \leq j \leq m, 1 \leq k \leq d_j\}$ constructed in the next algorithm is a basis for W

6.3.9: Let $\mathcal{B}$ be the ordered basis of W - $\{\vec{v}_{j,k} : 1 \leq j \leq m, 1 \leq k \leq d_j\}$. Then ${}_\mathcal{B}[\psi]_\mathcal{B} =$

$$\operatorname{diag} \underbrace{J(m), .., J(m)}_{d_m \text{ times}}, \underbrace{J(m-1), .., J(m-1)}_{d_{m-1} - d_m \text{ times}}, .., \underbrace{J(1), .., J(1)}_{d_1 - d_2 \text{ times}}$$

where $J(r)$ denotes the nilpotent Jordan block of size r

Theorem 6.3: JNF Basis Algorithm

Algorithm to construct a basis for each W_i/W_{i-1}:

- Choose an arbitrary basis for W_m/W_{m-1}, say

$$\{v_{m,1} + W_{m-1}, \vec{v}_{m,2} + W_{m-1}, \ldots, \vec{v}_m, d_m + W_{m-1}\}$$

- Since $\psi_m : W_m/W_{m-1} \to W_{m-1}/W_{m-2}$ is injective by 6.3.6, 6.3.7 proves that

$$\{\psi(\vec{v}_{m,1}) + W_{m-2}, \psi(\vec{v}_m, 2) + W_{m-2}, .., \psi(\vec{v}_m, d_m + W_{m-2})\}$$

is a linearly independent set in W_{m-1}/W_{m-2}. Set $\vec{v}_{m-1,i} = \psi(\vec{v}_{m,i})$ for $1 \leq i \leq d_m$

- Choose vectors $\{\vec{v}_{m-1,i} : d_m + 1 \leq i \leq d_{m-1}\}$ so that $\{\vec{v}_{m-1,i} + W_{m-i-1} : 1 \leq k \leq d_{m-i}\}$ is a basis of W_{m-1}/W_{m-2}

- Repeat!

6.3 PageRank, again

Theorem 6.5.1

If $M \in \operatorname{Mat}(n; \mathbb{R})$ is a Markov matrix with all positive entries, consider M as a complex matrix whose entries just happen to be real. If $\lambda \in \mathbb{C}$ is an eigenvalue of M then either $\lambda = 1$ or $|\lambda| < 1$

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.
Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.