

Honours Algebra Exam Notes

Made by Leon :) *Note: Any reference numbers are to the lecture notes*

1 Abstractions upon Abstractions

Definition A: Rings and Fields

A **ring** (left) is a set with two operations $(\mathbb{R}, +, \cdot)$ that satisfies the following lemmas.

A **field** (right) is an extension of a ring where (\cdot) is a group

1. $(R, +)$ is an abelian group with identity 0

2. (R, \cdot) is a **monoid**, i.e. it is a set with **Associativity** and **Identity** (written as 1)

3. **Distributive law:** For all a, b , and c in F , we have

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

and they satisfy the following lemmas (for both):

1. $0a = 0 = a0$

2. The elements 0 and 1 are distinct (only ring case is zero ring)

1. $(F, +)$ is an abelian group F^+ , with identity 0_F

2. $(F \setminus \{0_F\}, \cdot)$ is an abelian group F^\times , with identity 1_F

3. **Distributive law:** For all a, b , and c in F , we have

$$a(b + c) = ab + ac \in F$$

Field Specific Lemmas:

1. (\cdot) in F is associative, 1_F is an identity (it's an abelian group only in $(F \setminus \{0_F\}, \cdot)$)

Ring Specific Lemmas and Definitions:

1. The **null ring** or **zero ring** is defined as a ring where R is a single element - i.e. $\{0\}$ where $0 + 0 = 0$ and $0 \times 0 = 0$
2. A **commutative ring** is one where $a \cdot b = b \cdot a$ for all $a, b \in R$
3.

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

$m(na) = (mn)a$

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

$m(ab) = (ma)b = a(mb)$

$m(a + b) = ma + mb$

$(ma)(nb) = (mn)(ab)$

$(m + n)a = ma + na$

Definition B: Modules and Vector Spaces

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

A **vector space** V over a field F (*right*) is an extension of a module but over a field instead, and using vectors - $V = (V, +)$

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

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

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

Distributivity 1

Distributivity 2

Associativity

Identity

$\lambda(\vec{v} + \vec{w}) = \lambda\vec{v} + \lambda\vec{w}$

$(\lambda + \mu)\vec{v} = \lambda\vec{v} + \mu\vec{v}$

$\lambda(\mu\vec{v}) = (\lambda\mu)\vec{v}$

$1\vec{v} = \vec{v}$

and they satisfy the following lemmas (for both):

1. $0_R a = 0_M$ for all $a \in M$

or

$0\vec{v} = \vec{0}$ for all $\vec{v} \in V$

2. $r0_M = 0_M$ for all $r \in R$

or

$\lambda\vec{0} = \vec{0}$ for all $\lambda \in F$

$(-r)a = r(-a) = -(ra)$ for all $r \in R, a \in M$

$(-1)\vec{v} = -\vec{v}$ for all $\vec{v} \in V$

Definition C: Sub-things

A sub-thing is basically something that is a smaller but self-contained version of a thing

Vector Subspace (*left*): A subset U of a vector space V

Subring (*centre*): A subset R' of a ring R under the same operations of addition and multiplication defined in R

Submodule (*right*): A subset M' of a module M under the same operations of the R -module M **restricted to** M

Subspace Criterion	Subring Criterion	Submod. Criterion
$\forall \vec{u}, \vec{v} \in U, \lambda \in F$	$\forall a, b \in R'$	$\forall a, b \in M', r \in R$
1. $\vec{0} \in U$	1. R' has a multiplicative identity	1. $0_M \in M'$
2. $\vec{u} + \vec{v} \in U$	2. $a - b \in R'$	2. $a - b \in M'$
3. $\lambda \vec{u} \in U$	3. $a \cdot b \in R'$	3. $ra \in M'$

Definition D: Homo no homo

Everything has its own homomorphism and they are all the same thing

Linear Mapping (*left*): Homomorphism on a Vector Space

Ring Homomorphism (*centre*): Homomorphism on a ring

R-homomorphism (*right*): Homomorphism on a module

V. Space Criterion
 $\forall \vec{u}, \vec{v} \in U, \lambda \in F$

Ring Criterion
 $\forall x, y \in R'$

Module Criterion
 $\forall a, b \in M', r \in R$

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

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

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

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

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

$f(ra) = rf(a)$

A bijective homomorphism is called a **isomorphism**

Two objects with an iso. are called **isomorphic**, written $A \cong B$

A homomorphism $V \rightarrow V$ is called an **endomorphism** of V

An isomorphism $V \rightarrow V$ is called an **automorphism** of V

Properties of ring homos: Let R and S be rings and $f : R \rightarrow S$ a ring homomorphism. Then $\forall x, y \in R$ and $m \in \mathbb{Z}$ ($0_R, 0_S$ are the zeros of R, S):

1. $f(0_R) = 0_S$

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 $n \in \mathbb{N}$

Image and Kernel

The image and kernel of a mapping $f : M \rightarrow N$ are as follows:

Image: $\text{im } f = \{f(a) : a \in M\} \subseteq N$

Kernel: $\ker f = \{a \in M : f(a) = 0_N\} \subseteq M$

Definition 3.4: Ideals and Submodules

Def 3.4.7: $I \subseteq R$ 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 $ri, ir \in I$

Def 3.4.11: R be a commutative ring and let $T \subseteq R$. Then the **ideal of R generated by T** is the set

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

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

Submodule extra defs and conditions

Submods add the zero element in the case $T = \emptyset$.

If $T = \{t_1, \dots, t_n\}$, a finite set, we write $_{R}\langle t_1, \dots, t_n \rangle$ instead of $_{R}\{t_1, \dots, t_n\}$.

M is **finitely generated** if it's generated by a finite set $M = _R\langle t_1, \dots, t_n \rangle$.

M is **cyclic** if it's generated by a singleton $M = _R\langle T \rangle$

Def 3.4.15: 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: Ideals and Submodule Theorems/Lemmas

Let R, S be rings, and let $f : R \rightarrow S$ a ring-homomorphism

3.4.14: Let $T \subseteq R$. Then $_{R}\langle T \rangle$ is the smallest ideal of R that contains T

3.4.18 $\ker f$ is an ideal of R (but $\text{im } f$ is not always an ideal of S).

3.4.20: f is injective iff $\ker f = \{0\}$

3.4.21: The intersection of any collection of submodules of M is a submodule of M

3.4.22: Let I and J be ideals of R

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

is an ideal of R

Let R be a ring, M, N be modules, and $f : M \rightarrow N$ a R -homomorphism

3.7.28: Let $T \subseteq M$. Then $_{R}\langle T \rangle$ is the smallest submodule of M that contains T

3.7.21: $\ker f$ is a submodule of M , and $\text{im } f$ is a submodule of N

3.7.22: f injective iff $\ker f = \{0_M\}$

3.7.29: The intersection of any collection of submodules of M is a submodule of M .

3.7.30: Let M_1 and M_2 be submodules of M . Then

$$M_1 + M_2 = \{a + b : a \in M_1, b \in M_2\}$$

is a submodule of M

Definition 3.5.1: 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 $yRz \implies xRz$

Suppose that is an equivalence relation on a set X .

Equivalence class of x : $E(x) := \{z \in X : z \sim x \text{ for } x \in X\}$

Equivalence class for \sim : $E \subseteq X$, if $\exists x \in X$ s.t. $E = E(x)$

Representative: Element of an equivalence class

System of representatives for \sim : A subset $Z \subseteq X$ containing precisely one element from each equivalence class

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 $\text{can} : X \rightarrow (X / \sim), x \mapsto E(x)$ (surjection)

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

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

Thm 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 and multiplication is defined by

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

Def 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 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:

$$(a + N) + (b + N) = (a + b) + N$$
$$r(a + N) = ra + N$$

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 $a + N$ is the coset $-(a + N) = (-a) + N$
The R -module M/N is the **factor module** of M by the submod. N

Theorem E: Universal Properties and First Iso Thm

Thm: Universal Properties

Let A be an object of type σ , and I be an ideal-ish σ object

The mapping $\text{can} : A \rightarrow A/I$ sending a to $a + I$ for all $a \in A$ is a surjective σ -homomorphism with kernel I

If $f : A \rightarrow B$ is an σ -homomorphism with $f(I) = \{0_B\}$, so that $I \subseteq \ker f$, then there is a unique σ -homomorphism $\bar{f} : A/I \rightarrow B$ such that $f = \bar{f} \circ \text{can}$

Thm: First Isomorphism Theorem

Every σ homomorphism $f : A \rightarrow B$ induces an σ -isomorphism

$$\bar{f} : A / \ker f \xrightarrow{\sim} \text{im } f$$

This can be applied to pretty much everything!

Factor Rings: σ are rings (so A is a ring), and I is an ideal

Factor Modules: σ are R -modules, and I is a submodule

Groups: σ are groups, and I is a normal subgroup

2 Rings and Modules

Example 3.1.4: Modulo Rings

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

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

The elements of $\mathbb{Z}/m\mathbb{Z}$ consist of **congruence classes** of integers modulo m , written \bar{a} , - i.e. “the subsets T of \mathbb{Z} of the form $T = a + m\mathbb{Z}$ with $a \in \mathbb{Z}$ ”, or “set of integers that have the same remainder when you divide them by m ”. $\bar{a} = \bar{b}$ is the same as $a - b \in m\mathbb{Z}$, and often I’ll write

$$a \equiv b \pmod{m}$$

Thm 3.1.11 - Prime Property for Fields: Let $m \in \mathbb{N}$. The commutative ring $\mathbb{Z}/m\mathbb{Z}$ is a field iff and only if m is prime

Definition 3.2.3: 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 $(-m)a = -(ma)$

Definition 3.2: Units and Field Construction

Def 3.2.6: Let R be a ring. An element $a \in R$ is called a **unit** if it is invertible in R , i.e. there exists $r^{-1} \in R$ such that

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

Prop 3.2.9: The set of R^\times units in a ring R forms a group under multiplication

Definition 3.1.8: A **field** is a non-zero commutative ring F in which every non-zero element $a \in F$ is a unit.

Definition 3.2.11: zero-divisors of a ring

In a ring R , a non-zero a is called a **zero-divisor** or **divisor of zero** if there exists a non-zero element b such that either $ab = 0$ or $ba = 0$.

3.2.12 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 $b \neq 0 \implies ab \neq 0$

Recall A: Group

- Closure: $a * b \in G$
- Associativity: $(a * b) * c = a * (b * c)$
- Identity: $\exists e$ s.t. $e * g = g * e = e$
- Inverse: $\exists g$ s.t. $g * g^{-1} = g^{-1} * g = e$

Theorem 3.2: Integral Domain Properties

3.2.15 (Cancellation Law): Let R be an integral domain and let $a, b, c \in R$. If $ab = ac$ and $a \neq 0$ then $b = c$

3.2.16 Let m be a natural number. Then $\mathbb{Z}/m\mathbb{Z}$ is an integral domain iff and only if m is prime.

3.2.17 Every **finite** integral domain is a field.

Definition 3.1.1: 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 **quadratic**, and degree three is called **cubic**.

Thm 3.3.2: 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: Properties of a Polynomial Ring

- 3.3.3:** 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 $R[X]$
- 3.3.4:** 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 $B = 0$

Theorem 3.3.10: Degrees of Polynomial Roots

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

Definition 3.3.6: Evaluating a Function

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

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

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

Definition 3.3.11: Algebraically closed fields

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

Thm 3.3.13 (Fundamental Thm of Algebra): The field of complex numbers \mathbb{C} is algebraically closed.

Thm 3.3.14 (Linear factors of closed fields): If F is an algebraically closed field, then every non-zero polynomial $P \in F[X] \setminus \{0\}$ **decomposes into linear factors**

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

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

3 Linear algebra (ew)

Definition 1.4.5: 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 $\alpha_1, \dots, \alpha_r \in F$ and $\vec{v}_1, \dots, \vec{v}_r \in T$, together with the zero vector in the case $T = \emptyset$ ”

Terminology Dump

- **Linear Combination** of vectors $\vec{v}_1, \dots, \vec{v}_r$: An expression of the form $\alpha_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r$
 - **Vec. Subspace generated(or spanned) by T / span of T :** The smallest vector subspace $\langle T \rangle \subseteq V$ containing 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
- 1.4.7: Generating / Spanning set:** A subset of a vector space that spans the entire space. A vector space that has a finite generating set is said to be **finitely generated**
- 1.5.8: Basis of a vec space V :** a linearly independent generating set in V
- 1.5.9:** Let A and I be sets. A **family of elements of A indexed by I** , written $(a_i)_{i \in I}$ is a mapping $I \rightarrow A$

Theorem 1.5.11: Basis Theorems

Thm 1.5.11 (Linear combinations of basis elements): Let F be a field, V a vector space over F and $\vec{v}_1, \dots, \vec{v}_r \in V$ vectors. The family $(\vec{v}_i)_{1 \leq i \leq r}$ is a basis of V iff the following “evaluation” mapping, or if we label the family as \mathcal{A} , written $\psi = \psi_{\mathcal{A}} : F^r \rightarrow V$,

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

is a bijection

Thm 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 $E \setminus \{\vec{v}\}$ 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 $\vec{v} \in V$

Thm 1.5.14 (Basis Characterisation Variant)

- 1. If $L \subset V$ is a linearly indep. subset and E is minimal over all generating sets of V where $L \subseteq E$, then E is a basis.
- 2. If $E \subseteq V$ is a generating set and if L is maximal amongst all linearly indep. sets of V where $L \subseteq E$, then L is a basis.

Thm 1.5.16 (Variant of Linear Combis of basis elements): 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

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

Theorem 1.6.1: 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

$$|L| \leq |E|$$

Definition 1.4 - 1.5: Random sets

Def 1.4.9: The set of all subsets $\mathcal{P}(X) = \{U : U \subseteq X\}$ of X is the **power set** of X , $\mathcal{P}(X)$ is referred to as a **system of subsets of X** . We can now define 2 new subsets - the **union** and **intersection**

$$\begin{aligned} \bigcup_{U \in \mathcal{U}} U &= \{x \in X : \text{there is } U \in \mathcal{U} \text{ with } x \in U\} \\ \bigcap_{U \in \mathcal{U}} U &= \{x \in X : x \in U \text{ for all } U \in \mathcal{U}\} \end{aligned}$$

Def 1.5.15: Let X be a set and F a field. The set $\text{Maps}(X, F)$ of all mappings $f : X \rightarrow F$ becomes an F -vector space with the operations of 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 called the **free vector space on the set X**

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

Theorem 1.6: Steinitz Exchange Theorem

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

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

Theorem 1.6: Cardinality of Bases and Dimension

Def 1.6.4: Let V be a finitely generated vector space. V has a finite basis, and any two bases of V also have the same number of elements

Def 1.6.5: The cardinality of a basis of a finitely generated vector space V is called the **dimension** of V , written $\dim V$.

Theorems

1.6.7 (Cardinality Criterion for Bases)

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

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

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

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

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

Definition 1.7.1: Random tidbits about Linear Mappings

Def 1.7.5: A point that is sent to itself by a mapping is called a **fixed point** of the mapping. Given a mapping $f : X \rightarrow X$, we denote the set of fixed points by

$$X^f = \{x \in X : f(x) = x\}$$

Def 1.7.6: Two vector subspaces V_1, V_2 of a vector space V are called **complementary** if addition defines a bijection

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

Example (Direct Sum): Given vector spaces V_1, \dots, V_n, W and linear maps $f_i : V_i \rightarrow W$ we can form a new mapping $f : V_1 \oplus \dots \oplus V_n \rightarrow W$ by $f(v_1, \dots, v_n) = f_1(v_1) + \dots + f_n(v_n)$. This is a bijection

$$\text{Hom}(V_1, W) \times \dots \times \text{Hom}(V_n, W) \xrightarrow{\sim} \text{Hom}(V_1 \oplus \dots \oplus V_n, W)$$

Taking $W = V$, we produce a vector iso. $V_1 \oplus V_2 \xrightarrow{\sim} V$. Writing $V = V_1 \oplus V_2$, we call V the **direct sum**, or **internal direct sum** of the subspaces V_1, V_2

Theorem 1.7: Vector Spaces and Linear Maps

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

1.7.8 (Linear Mapping and Bases): Let V, W be vector spaces over a field F . The set of all homoms $V \rightarrow W$ is denoted by

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

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

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

1.7.9: (Inverse Mappings)

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

1.8.2 A linear mapping is injective iff its kernel is zero

1.8.4 (Rank-Nullity Theorem): Let $f : V \rightarrow W$ be a linear mapping between vector spaces. Then:

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

Dim. of $\text{im } f = \text{rank}$ of f , and the dim. of $\ker f = \text{nullity}$ of f

Theorem 2.1.1: Linear Maps $F^m \rightarrow F^n$ and Matrices

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

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

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

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

Theorem 2.1.8: Composition of maps to products

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

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

Definition 2.2: Big def-thm pairs

Thm 2.2.3: Every square matrix with entries in a field can be written as a product of elementary matrices

Def 2.2.4: Smith Normal Form: A matrix that is fully zero, except for 1's on the diagonal followed by 0's

Thm 2.2.5: 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 NF

Thm 2.4.5: Let $f : V \rightarrow W$ 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 ${}_B[f]_{\mathcal{A}}$ is in Smith Normal Form

Def 2.2.9: Rank of a matrix $A \in \text{Mat}(n \times m; F)$, written $\text{rk } A$: The dim. of the subspace of F^n generated by the columns of A , or same with the row (The row/column rank are the same). If the rank is equal to the no. of rows/columns, then the matrix has **full rank**

Def 2.4.6: Trace, written $\text{tr}(A)$ is the sum of diagonal entries

Theorem 2.3: Representing Matrices

Thm 2.3.1: Let F be a field, V and W vector spaces over F with ordered bases $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_m)$ and $\mathcal{B} = (\vec{w}_1, \dots, \vec{w}_n)$. Then to each linear mapping $f : V \rightarrow W$ we associate a **representing matrix** ${}_B[f]_{\mathcal{A}}$ whose entries a_{ij} are defined by the identity

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

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

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

Thm 2.3.2: Let F field and U, V, W finite dim. vector spaces over kF with ordered bases $\mathcal{A}, \mathcal{B}, \mathcal{C}$. If $f : U \rightarrow V, g : V \rightarrow W$ are linear maps, then the representing matrix of the composition $g \circ f : U \rightarrow W$ is the matrix product of the representing matrices of f and g :

$${}_C[g \circ f]_{\mathcal{A}} = {}_C[g]_{\mathcal{B}} \circ {}_B[f]_{\mathcal{A}}$$

Def 2.3.4: Let V be a finite dimensional vector space with an ordered basis $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_m)$. We'll denote the inverse to the bijection in 3

“ $\Phi_{\mathcal{A}} : F^m \xrightarrow{\sim} V, (\alpha_1, \dots, \alpha_m)^T \mapsto \alpha_1\vec{v}_1 + \dots + \alpha_m\vec{v}_m$ ” 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 2.3.4: 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 $f : V \rightarrow W$ be a linear mapping. The following holds for $\vec{v} \in V$:

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

Definition 2.4.1: Change of Basis Matrix

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

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

is called a **change of basis matrix**. Its entries are $\vec{v}_j = \sum_{i=1}^n a_{ij}\vec{w}_i$

Thm 2.4.3: Let V and W be finite dimensional vector spaces over F and let $f : V \rightarrow W$ be a linear mapping. Suppose that $\mathcal{A}, \mathcal{A}'$ are ordered bases of V and $\mathcal{B}, \mathcal{B}'$ are ordered bases of W . Then

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

Cor 2.4.4: Let V be a finite dimensional vector space and let $f : V \rightarrow V$ be an endomorphism of V . Suppose that $\mathcal{A}, \mathcal{A}'$ are ordered bases of V . Then

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

Definition 4.1.1: Symmetric Groups

The group of all permutations of the set $\{1, 2, \dots, n\}$, or bijections from $\{1, 2, \dots, n\}$ to itself is denoted by S_n and called the **n -th symmetric group**. It is a group under composition and has $n!$ elements.

• **Transposition:** A permutation that swaps two elements of the set and leaves all the others unchanged.

• **Inversion** of a permutation $\sigma \in S_n$: A pair (i, j) such that $1 \leq i < j \leq n$ and $\sigma(i) > \sigma(j)$.

• **Length** of σ : Num. of inversions of the perm. σ , written $\ell(\sigma)$. i.e.

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

• **Sign** of σ : The parity of the number of inversions of σ . i.e.:

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

Theorem 4.1: Multiplicativity of the sign

Thm 4.1.5: For each $n \in \mathbb{N}$, the sign of a permutation produces a group homomorphism $\text{sgn} : S_n \rightarrow \{+1, -1\}$ from the symmetric group to the two-element group of signs. In formulas:

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

Def 4.1.6 (Alternating Group): For $n \in \mathbb{N}$, the set of even permutations in S_n forms a subgroup of S_n because it's the kernel of the group homomorphism $\text{sgn} : S_n \rightarrow \{+1, -1\}$, written A_n

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 $H : U \times V \rightarrow W$ 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 $\lambda \in F$:

$$H(u_1 + u_2, v_2) = H(u_1, v_2) + H(u_2, v_2), \quad H(\lambda u_1, v_1) = \lambda H(u_1, v_1) \\ H(u_1, v_2 + v_2) = H(u_1, v_2) + H(u_1, v_2), \quad H(u_1, \lambda v_1) = \lambda H(u_1, v_1)$$

A bilinear form H is **symmetric** if $H(u, v) = H(v, u)$ 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 4.3.3: Multilinear Forms

Let V_1, \dots, V_n, W be F -vector spaces. A mapping $H : V_1 \times V_2 \times \dots \times V_n \rightarrow W$ is a **multilinear form** or just **multilinear** if for each j , the mapping $V_j \rightarrow W$ defined by $v_j \mapsto H(v_1, \dots, v_j, \dots, v_n)$, 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 $H : V \times \dots \times V \rightarrow W$ is **alternating** if it vanishes on every n -tuple of elements of V that has at least two entries equal, in other words if:

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

Theorem 4.3.6: Characterisation of the Determinant

Let F be a field. The mapping

$$\det : \text{Mat}(n; F) \rightarrow F$$

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

Definition 4.4.6: Cofactors of a Matrix

Let $A \in \text{Mat}(n; R)$ 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** (left) and similarly, the **j -th column expansion of the determinant** (right) is

$$\det(A) = \sum_{j=1}^n a_{ij} C_{ij} \quad \left| \quad \det(A) = \sum_{i=1}^n a_{ij} C_{ij} \right.$$

Definition 4.4.8: Adjugate Matrix

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

Theorem 4.4: Determinant Theorem Bank

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

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

4.4.9 (Cramer's Rule): Let A be a $(n \times n)$ -matrix with entries in a commutative ring R . Then

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

4.4.11 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, $A \in \text{Mat}(n; R)$ is invertible if and only if $\det(A) \in R^\times$

4.4.14 (Jacobi's Formula): Let $A = (a_{ij})$ where the coefficients $a_{ij} = a_{ij}(t)$ are functions of t . Then

$$\frac{d}{dt} \det A = \text{Tr} \text{Adj} A \frac{dA}{dt}$$

Definition 4.5.6: Characteristic Polynomial

Let R be a commutative ring and let $A \in \text{Mat}(n; R)$ 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

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

Thm: 4.5.8: Let F be a field and $A \in \text{Mat}(n; F)$ a square matrix with entries in F . The eigenvalues of the linear mapping $A : F^n \rightarrow F^n$ are exactly the roots of the characteristic polynomial χ_A

Theorem 4.5.9: Eigenvalue Remarks

- Thm 4.5.4 (Existence of Eigenvalues)** Each endomorphism of a non-zero finite dimensional vector space over an algebraically closed field has an eigenvalue
- Square matrices $A, B \in \text{Mat}(n; R)$ of same size are **conjugate** if

$$B = P^{-1}AP \in \text{Mat}(n; R)$$

for an invertible $P \in GL(n; R)$

- Conjugacy is an equivalence relation on $\text{Mat}(n; R)$
- The char. polynomials for two conjugate matrices are the same
- We can define the char. polynomials of an endomorphism $f : V \rightarrow V$ of an n -dim vector space over a field F to be

$$\chi_f(x) = \chi_A(x) \in F[x]$$

with $A = {}_{\mathcal{A}}[f]_{\mathcal{A}} \in \text{Mat}(n; R)$ 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 $f : V \rightarrow V$ 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:

$$g : W \rightarrow W; \vec{w} \mapsto f(\vec{w})$$

$$h : V/W \rightarrow V/W; W + \vec{v} \mapsto W + f(\vec{v})$$

The char. poly. of f is the product of the char. poly.s of g and h

Definition 4.6.1: Triangularisability

Let $f : V \rightarrow V$ be an endomorphism of a finite dimensional F -vector space V . f is **triangularisable** if the vector space V has an ordered basis $\mathcal{B} = (\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n)$ such that

$$f(\vec{v}_1) = a_{11}\vec{v}_1,$$

$$f(\vec{v}_2) = a_{12}\vec{v}_1 + a_{22}\vec{v}_2,$$

$$\vdots$$

$$f(\vec{v}_n) = a_{1n}\vec{v}_1 + a_{2n}\vec{v}_2 + \dots + a_{nn}\vec{v}_n \in V$$

(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 ${}_B[f]_B = (a_{ij})$ representing f with respect to \mathcal{B} is upper triangular (or any other triangular)

Theorem 4.6.1 - 4.6.3

Let $f : V \rightarrow V$ 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

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

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

An endomorphism $A : F^n \rightarrow F^n$ 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 $f : V \rightarrow V$ 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 $\mathcal{B} = \{\vec{v}_1, \dots, \vec{v}_n\}$ where ${}_B[f]_B = \text{diag}(\lambda_1, \dots, \lambda_n)$. In this case, of course, $f(\vec{v}_i) = \lambda_i \vec{v}_i$.

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

Theorem 4.6.9: Linear Independence of Eigenvectors

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

Theorem 4.6.10: Cayley-Hamilton Theorem

Let $A \in \text{Mat}(n; R)$ 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 Inner Product Spaces

Definition 5.1.1: Inner Product

Let V be a vector space over \mathbb{R} . An **inner product** on V is a mapping

$$(_, _) : V \times V \rightarrow \mathbb{R}$$

that satisfies the following for all $\vec{x}, \vec{y}, \vec{z} \in V$ and $\lambda, \mu \in \mathbb{R}$:

- $(\lambda\vec{x} + \mu\vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})$
- $(\vec{x}, \vec{y}) = (\vec{y}, \vec{x})$
- $(\vec{x}, \vec{x}) \geq 0$, 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 \bar{z} is the complex conjugate

Definition 5.1.5: Norm

In a real/complex inner product space, the **length** or **inner product norm** or **norm** $\|\vec{v}\| \in \mathbb{R}$ of a vector \vec{v} is 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 space V satisfies, for any $\vec{v}, \vec{w} \in V$ and scalar λ :

- $\|\vec{v}\| \geq 0$ with equality iff $\vec{v} = \vec{0}$
- $\|\lambda\vec{v}\| = |\lambda| \|\vec{v}\|$
- $|\vec{v} + \vec{w}| \leq \|\vec{v}\| + \|\vec{w}\|$ (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. If $\delta_{i,j}$ is the **Kronecker delta** defined by "1 if $i = j$, and 0 otherwise", this 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

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 Othogonals

Let V be an inner product space and let U be a finite dimensional subspace of V . Then U and U^\perp are complementary, 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

$$\pi_U : V \rightarrow V$$

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 $\vec{v} \in V$

$$\pi_U(\vec{v}) = \sum_{i=1}^n \langle \vec{v}, \vec{v}_i \rangle \vec{v}_i$$

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

$$|\langle \vec{v}, \vec{w} \rangle| \leq \|\vec{v}\| \|\vec{w}\|$$

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 $1 \leq i \leq k$,

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

Gram-Shmidt Algorithm: Start with an arbitrary linerly independent ordered subset v_1, v_2 of an inner product space

1. Take the first element v_1 and normalise it to have length 1
2. Take v_2 , and subtract the orthogonal projection of it to the space $\langle \vec{w}_1 \rangle$ to make it a right angle. Normalise this to have length 1
3. Take v_3 and subtract the orthogonal projection of it onto $\langle \vec{w}_1, \vec{w}_2 \rangle$. Normalise this to length 1

Repeat this for all vectors. Observe that for each step we have $\langle \vec{w}_{i-1}, \dots, \vec{w}_1 \rangle \subseteq \langle \vec{v}_{i-1}, \dots, \vec{v}_1 \rangle$ and because the dimension of both sides is the same, it's actually an equality

Definition 5.3.1: Adjoints

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

$$\langle T\vec{v}, \vec{w} \rangle = \langle \vec{v}, S\vec{w} \rangle$$

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 $T : V \rightarrow V$ be an endomorphism. Then T^* exists. That is, there is a unique linear mapping $T^* : V \rightarrow V$ such that for all $\vec{v}, \vec{w} \in V$:

$$\langle T\vec{v}, \vec{w} \rangle = \langle \vec{v}, T^*\vec{w} \rangle$$

Definition 5.3.5: Self Adjoints

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

Thm 5.3.7: Let $T : V \rightarrow V$ 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 $\langle \vec{v}, \vec{w} \rangle = 0$
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 $P^{-1} = P^T$

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 $T : V \rightarrow V$ 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

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

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

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

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

5 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 $\phi : V \rightarrow V$ be an endomorphism of V with char. polynomial

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

For distinct $\lambda_1, \lambda_2, \dots, \lambda_s \in F$. 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, $_{\mathcal{B}}[\phi]_{\mathcal{B}}$

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

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

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

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 :

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

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

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

$E^{\text{gen}}(\lambda_i, \phi) \subseteq E^{\text{gen}}(\lambda_i, \phi)$, 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 $f : X \rightarrow X$ 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: JNF Theorem Bank

6.3.6: For each i , define a linear mapping

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

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 $f : X \rightarrow Y$ be an injective linear mapping between the F -vector spaces X and Y . If $\{\vec{x}_1, \dots, \vec{x}_t\}$ is a linearly independent set in X , then $\{f(\vec{x}_1), \dots, f(\vec{x}_t)\}$ 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 $_{\mathcal{B}}[\psi]_{\mathcal{B}} =$

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

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

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

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

3. Then

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

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

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

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

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 $\{v_{m,1} + W_{m-1}, \vec{v}_{m,2} + W_{m-1}, \dots, \vec{v}_m, d_m + W_{m-1}\}$
- Since $\psi_m : W_m/W_{m-1} \rightarrow W_{m-1}/W_{m-2}$ is injective by 6.3.6, 6.3.7 proves that $\{\psi(\vec{v}_{m,1}) + W_{m-2}, \psi(\vec{v}_{m,2}) + W_{m-2}, \dots, \psi(\vec{v}_m, d_m + W_{m-2})\}$ 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!