1 Vector Spaces

1.1 Fields and Vector Spaces

Recall A: Definition of a Group

For an operation $*$, We say a non-empty set G is a **group** under $*$ if the following four axioms hold:

- **G1 - Closure:** $a * b \in G$ for all $a, b \in G$.
- **G2 - Associativity:** $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
- **G3 - Identity:** There exists an *identity* element of G such that $e * g = g * e = g$ for all $g \in G$.
- **G4 - Inverse:** Every element $g \in G$ has an *inverse* g^{-1} such that $g * g^{-1} = g^{-1} * g = e$

An **Abelian Group** is one where $a * b = b * a$ (commutative)

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

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

2 Rings

I can't be bothered doing changes of basis and stuff, time for something more interesting :D

2.1 Ring basics

Definition 2.1.1: 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** - this means that the second operation $\cdot : R \times R \to R$ is associative and that there is an **identity element** $1 = 1_R \in R$, often just called the identity, with the property that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.
3. The distributive laws hold, meaning that for all $a, b, c \in R$,
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c))$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

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'll call the element $1 \in R$ as the identity element of the monoid $(R, \cdot)$, and we call the additive identity of $(R, +)$ zero, written as 0_R or 0
Example: We can define the **null ring** or **zero ring** as a ring where R is a single ement set, e.g. $\{0\}$, with the operations $0 + 0 = 0$ and $0 \times 0 = 0$. We will call any ring that isn't the zero ring a **non-zero ring**

Example 2.1.2: Modulo Rings

Let $m \in \mathbb{Z}$ be an integer. 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

$$a \equiv b \mod m$$

2.2 Linking Rings to Fields and Further Properties

Definition 2.2.1: 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 $a \cdot a^{-1} = a^{-1} \cdot a = 1$

Theorem 2.2.2: Prime property of fields

Let m be a positive integer. The commutative ring $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime.

Theorem 2.2.3: Lemmas for multiplying

Let R be a ring and let $a, b \in R$. Then

1. $0a = 0 = a0$
2. $(-a)b = -(ab) = a(-b)$
3. $(-a)(-b) = ab$

Definition 2.2.4: 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 2.2.5: Lemmas for multiples

Let R be a ring, let $a, b \in R$ and let $m, n \in \mathbb{Z}$. Then:

1. $m(a + b) = ma + mb$
2. $(m + n)a = ma + na$
3. $m(na) = (mn)a$
4. $m(ab) = (ma)b = a(mb)$
5. $(ma)(nb) = (mn)(ab)$

Definition 2.2.6: 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

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

Theorem 2.2.7

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

Definition 2.2.8: 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 $ba = 0$.

Theorem 2.2.9: Cancellation Law

Let R be an *integral domain* and let $a, b, c \in R$. If $ab = ac$ and $a \neq 0$ then $b = c$

Theorem 2.2.10: Prime Property for Integral Domains

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

Theorem 2.2.11

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

2.3 Polynomials

Definition 2.3.1: Polynomial

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

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

for some non-negative integer m 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**, a polynomial od degree two is called **quadractic**, and a polynomial of degree three is called **cubic**.

Definition 2.3.2: 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 2.3.3: Zero-Divisors 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 $R[X]$

Theorem 2.3.4: Division and Remainder

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

Definition 2.3.5: Formal definition of a function

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

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

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

Theorem 2.3.6: Roots of a Polynomial

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 2.3.7: 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 2.3.8: 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 2.3.9: Fundamental Theorem of Algebra

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

Theorem 2.3.10: 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 Determinants and Eigenvalues Redux

3.1 Symmetric Groups

Definition 3.1.1: 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 3.1.2: 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:

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

Theorem 3.1.3: Multiplicativity of the sign

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

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

Definition 3.1.4: 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 $\mathrm{sgn} : S_n \to \{+1, -1\}$. This group is the **alternating group** and is denoted A_n

3.2 Determinants

Definition 3.2.1: Determinants

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

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

3.3 Characterising the Determinant

Definition 3.3.1: 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 $\lambda \in F$:

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

Definition 3.3.2: 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.

Definition 3.3.3: Alternating Multilinear Forms

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 3.3.4: 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

3.4 Rules for Calculating with Determinants

Theorem 3.4.1: Multiplicativity of the Determinant

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

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

Theorem 3.4.2

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

3.4.3 Consequences of determinant rules

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

Theorem 3.4.4: Determinants of a Transpose Matrix

The determinant of a square matrix and of the transpose of the square matrix are equal, that is for all $A \in \mathrm{Mat}(n; R)$ with R a commutative ring,

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

Definition 3.4.5: Cofactors of a Matrix

Let $A \in \mathrm{Mat}(n; R)$ for some commutative ring R and natural number n. Let i and j be integers between 1 and n. Then the $(i,)$ **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 3.4.6: 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 3.4.7: 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 3.4.8: Cramer's Rule

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

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

3.4.9 Alternative Definition of Cramer's

In many sources, such as Wikipedia, Cramer's Rule means the formula

$$x_i = \frac{\det(a_{*1} \mid \cdots \mid b_* \mid \cdots \mid a_{*n})}{\det(a_{*1} \mid \cdots \mid a_{*i} \mid \cdots \mid a_{*n})}$$

for solving a field F the system $A\vec{x} = \vec{b}$ of n linear equations in n unknowns, provided that a unique solution exists. A unique solution exists if and only if A is invertible. So, instead of applying the Gaussian algorithm, you can calculate lots of determinants, replacing the i-th column of A by the given solution vector $\vec{b}$. It turns out that if you implement this rule on a computer, it has the same efficiency as the Gaussian algorithm. The relationship between this version of Cramer's rule and the above theorem is got by successively taking the vector $\vec{b}$ in the system of linear equations to be the standard basis elements $\vec{e_i}$ with $1 \le i \le n$.

Theorem 3.4.10: 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 $\det(A) \in R^\times$

So for instance, an integral matrix $A \in \mathrm{Mat}(n; \mathbb{Z})$ is invertible if and only if $\det(A)$ is 1 or -1, since $\mathbb{Z}^\times = \{\pm 1\}$. On the other hand, a matrix $A \in \mathrm{Mat}(n; F)$ with entries in a field F is invertible if and only if $\det(A) \neq 0$ since $F^\times$ consists of the non-zero elements of F.

Theorem 3.4.11: Jacobi's Formula

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

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

3.5 Eigenvalues and Eigenvectors

Definition 3.5.1: 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 3.5.2: Existence of Eigenvalues

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

Definition 3.5.3: 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 3.5.4: 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

3.5.5 Eigenvalue remarks

1. Square matrices $A, B \in \mathrm{Mat}(n; R)$ of the same size are *conjugate* if
$$B = P^{-1}AP \in \mathrm{Mat}(n; R)$$
for an invertible $P \in \mathrm{GL}(n; R)$. Conjugacy is an equivalence relation on $\mathrm{Mat}(n; R)$. (The definition makes sense for any commutative ring R, although we will mainly be concerned with the case of a field)

2. The motivation for conjugacy comes from the various matrix representations for an endomorphism $f : V \to V$ of an n-dimensional vector space V over a field F. Let
$$A = (a_{ij}) = {}_{\mathcal{A}}[f]_{\mathcal{A}},\ B = (b_{ij}) = {}_{\mathcal{B}}[f]_{\mathcal{B}} \in \mathrm{Mat}(n; f)]$$
be the matrices of f with respect to bases $\mathcal{A} = (\vec{v_1}, \vec{v_2}, \ldots, \vec{v_n})$, $\mathcal{B} = (\vec{w_1}, \vec{w_2}, \ldots, \vec{w_n})$ for V
$$f(\vec{v_j}) = \sum_{i=1}^{n} a_{ij}\vec{v_i},\ f(\vec{w_j}) = \sum_{i=1}^{n} b_{ij}\vec{w_i} \in V$$
The change of basis matrix $P = (p_{ij}) = {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{B}} \in \mathrm{Mat}(n; F)$ is invertible, with
$$\vec{w_j} = \sum_{i=1}^{n} p_{ij}\vec{v_i} \in V$$
We have the identity
$$B = P^{-1}AP \in \mathrm{Mat}(n; F)$$
so A, B are conjugate

3. **Key observation**: the characteristic polynomials of conjugate $A, B \in \mathrm{Mat}(n, R)$ are the same
$$\begin{aligned} \chi_B(x) = \det(xI_n - B) &= \det(xI_n = P^{-1}AP) \\ &= \det(P^{-1}(xI_n - A)P) = \det(P)^{-1}\det(xI_n - A)\det(P) \\ &= \det(xI_n - A) = \chi_A(x) \in R[x] \end{aligned}$$

4. In view of 2 and 3 we can define the characteristic polynomial of an endomorphism $f : V \to V$ of an n-dimensional vector space over a field F to be
$$\chi_f(x) = \chi_A(x) \in F[x]$$

with $A = \mathcal{A}[f]_\mathcal{A} \in \mathrm{Mat}(n; R)$ the matrix of f with respect to *any* basis $\mathcal{A}$ for V. Thanks to 3.5.4, the eigenvalues of f are exactly the roots of χ_f, the characteristic polynomial of f

Remark: 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

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

Any ordered basis $\mathcal{A} = (\vec{w_1}, \vec{w_2}, \dots, \vec{w_m})$ for W can be extended to an ordered basis for V

$$\mathcal{B} = (\vec{w_1}, \vec{w_2}, \dots, \vec{w_m}, \vec{v}_{m+1}, \vec{v}_{m+2} \cdots, \vec{v_n})$$

The images of the $\vec{v}_j$'s under the canonical projection can : $V \to V/W$ are then an ordered basis for V/W

$$\mathcal{C} = (\mathrm{can}(v_{m+1}), \mathrm{can}(v_{m+2}), \dots, \mathrm{can}(\vec{v}_n))$$

Let $a_{ij}, b_{jk}, c_{ik} \in F$ be the coefficients in the linear combinations

$$f(\vec{w}_j) = \sum_{i=1}^{m} a_{ij}\vec{w}_i \in W, \, f(\vec{v}_k) = \sum_{j=m+1}^{n} b_{jk}\vec{v}_j + \sum_{i=1}^{n} c_{ik}\vec{w}_i \in V$$

[WIP SO MUCH WRITING OMG]

3.6 Triangularisable, Diagonalisable, and Cayley-Hamilton

Definition 3.6.1: 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 $\mathcal{B} = (\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n)$ 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 3.6.2

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 $F[x]$

Theorem 3.6.3: Triangularisability and Conjugacy

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

Definition 3.6.4: Diagonalisability

An endomorphism $f: V \to V$ of an F-vector space V is **diagonalisable** if and only if 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 $\mathcal{B} = \{\vec{v}_1, \dots, \vec{v}_n\}$ such that corresponding matrix representing f is diagonal, that is ${}_\mathcal{B}[f]_\mathcal{B} = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$. In this case, of course, $f(\vec{v}_i) = \lambda_i\vec{v}_i$.
A square matrix $A \in \mathrm{Mat}(n; F)$ is **diagonalisable** if and only if the corresponding linear mapping $F^n \to F^n$ given by left multiplication by A is diagonalisable. Thanks to [something] this just means that A is conjugate to a diagonal matrix, there exists an invertible matrix $P \in \mathrm{GL}j(n; F)$ such that $P^{-1}AP = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$. 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 3.6.5: Linear Independence of Eigenvectors

Let $f: V \to V$ 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 3.6.6: 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.

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.
Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.
Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.
Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.
Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.
Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.
Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.
Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetuer a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et

ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consectetuer. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetuer odio sem sed wisi.

Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetuer eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris. Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.