1 Introduction

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.

1.1. Basic Definitions

Definition 1.1
A **field** $(k, +, \times)$ is a set with two operations:

- $(k, +)$ is an abelian group with identity 0,
- $(k^* = k - \{0\}, \times)$ is an abelian group with identity 1,
- Distributive law: $a\,(b + c) = ab + ab$.

Example 1.2
Some fields of characteristic 0, e.g. $\underbrace{1 + \ldots + 1}_{n} = n \cdot 1 \neq 0$, are $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. However, $\mathbb{F}_p = \mathbb{Z}/p$ with p prime have characteristic p.

Definition 1.3
A **vector space** over k is a set V with the following operations and properties:

- Addition: $+ \colon V \times V \to V$,
- $(V, +)$ is an abelian group with identity $0 \in V$,
- Scalar multiplication: $k \times V \to V$,
- $(ab)v = a(bv)$ for all $a, b \in k$ and $v \in V$ (associativity),
- $a(v + w) = av + aw$ for all $a \in k$ and $v \in V$ (distributivity).

A **subspace** is a set $W \subset V$ where $0 \in W$ and W is closed under $+, \times$.

Example 1.4
k^n, $k[x]$ (i.e. polynomials in k), et cetera.

Definition 1.5
The **span** of a set of vectors $v_1, \ldots, v_n$ is the subspace spanned by all $\{v_i\}$, i.e.

$$\operatorname{span}(v_1, \ldots, v_n) = \left\{ \sum a_i v_i \mid a_i \in k \right\} \subseteq V.$$

We say $\{v_i\}$ spans V if $\operatorname{span}(\{v_i\}) = V$.

Definition 1.6
Say $\{v_i\}$ are **linearly independent** if $a_1 v_1 + \ldots + a_n v_n = 0 \implies a_i = 0 \forall i$.

Definition 1.7
A **basis** is a set of linearly independent vectors $\{v_i\}$ which span V. Equivalently, we have an isomorphism

$$\begin{aligned} \text{basis} \colon k^n &\longrightarrow V \\ \{a_i\} &\longmapsto \sum a_i v_i. \end{aligned}$$

Theorem 1.8
All bases of V have the same cardinality $= \dim V$.

Corollary 1.9
Any linearly independent set $\{v_i\} \subseteq V$ can be completed to a basis.

Definition 1.10
The set $\operatorname{Hom}(V, W)$ of **linear maps** from V to W, with V, W vector spaces over k, is a vector space. Linear maps $\varphi \colon V \to W \in \operatorname{Hom}(V, W)$ satisfy $\varphi(u + v) = \varphi(u) + \varphi(v)$ and $\varphi(\lambda u) = \lambda \varphi(u)$.

Theorem 1.11 (Matrices)
Given bases $\{v_i\}$ and $\{w_j\}$ of V, W with $\dim V = n, \dim W = m$, represent $v = \sum x_i v_i$ by column vector $X = (x_1, \ldots, x_n)^t$ and $\varphi \in \operatorname{Hom}(V, W)$ by matrix $A = (a_{ij})$ whose columns represent $\varphi(v_j)$ in basis $\{w_j\}$, i.e. $\varphi(v_i) = \sum a_{ij} w_j$. Then $\varphi(v)$ is represented in basis w_j by column vector $Y = AX$. In other words, the following diagram commutes.

$$\begin{tikzcd} V \arrow[r, "\varphi"] & W \\ k^n \arrow[u, "basis"'] \arrow[r, "A"'] & k^m \arrow[u, "basis"'] \end{tikzcd}$$

Corollary 1.12 (Change of Basis)
*Given a **change of basis matrix** $P = (p_{ij}) = \mathcal{M}(\mathrm{id}, \{v_i'\}, \{v_i\})$, i.e. $v_j' = \sum p_{ij} v_i$, then for any $\varphi\colon V \to V$, we have $\mathcal{M}(\varphi, \{v_i'\}) = A' = P^{-1}AP$.*

Theorem 1.13
*We have an **direct sum decomposition** of V as $V \cong W_1 \oplus \ldots \oplus W_n$ if*

- *W_i span V: $\forall v \in V \exists w_i \in W_i s.t. v = w_1 + \ldots + w_n$,*
- *W_i are independent: $w_1 + \ldots + w_n = 0$, $w_i \in W_i \implies w_i = 0 \forall i$.*

Equivalently, $\varphi\colon \bigoplus W_i \to V$ with $\{w_i\} \mapsto \sum w_i$ is an isomorphism.

Corollary 1.14
Given V finite dimensional, $V = W_1 \oplus W_2$ iff $W_1 \cap W_2$ and $\dim W_1 + \dim W_2 = \dim V$.

Definition 1.15
For any $\varphi \in \mathrm{Hom}(V, W)$ for vector spaces V, W, we define

- the **kernel** of φ: $\ker\varphi = \{v \in V \mid \varphi(v) = 0\} \subseteq V$,
- the **image** of φ: $\operatorname{im}\varphi = \{w \in W \mid \exists v \in V, \varphi(v) = w\} \subseteq W$.

Theorem 1.16 (Rank-Nullity Theorem)
Given V, W finite dimensional, for any $\varphi \in \mathrm{Hom}(V, W)$ we have $\dim V = \dim\ker\varphi + \underbrace{\dim\operatorname{im}\varphi}_{=\operatorname{rank}\varphi}$.

Remark: There exists bases of $\{v_i\}$ of V, $\{w_j\}$ of W such that $\mathcal{M}(\varphi) = \begin{pmatrix} I_{r\times r} & 0 \\ 0 & 0 \end{pmatrix}$, where $r = \operatorname{rank}\varphi$ and $n - r = \operatorname{null}\varphi$.

1.2. Dual and Quotient Spaces

Definition 1.17
The **dual vector space** of V is defined as $V^* = \mathrm{Hom}(V, k)$.

Theorem 1.18
Given a basis of (finite dimensional) V $\{e_i\}$, there exists a dual basis $\{e_i^*\}$ of V^* such that $e_i^*(e_j) = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & else \end{cases}$.

Theorem 1.19 (Double Dual)
We have a natural isomorphism from V to $V^{**} = \mathrm{Hom}(V, V \to k)$ (for finite dimensional V)

given by

$$\begin{aligned} V &\longrightarrow V^{**} \\ v &\longmapsto \mathrm{ev}_v \colon (\ell \mapsto \ell(v)). \end{aligned}$$

If $\dim V = \infty$*, then this map is simply injective.*

Definition 1.20
The **annihilator** of $U \subseteq V$ is $\mathrm{Ann}(U) = \{\ell \in V^* \mid \ell(u) = 0 \, \forall u \in U\} \subseteq V^*$

Corollary 1.21
$\dim \mathrm{Ann}\, U = n - \dim U$.

Definition 1.22
The **transpose** of $\varphi \in \mathrm{Hom}(V, W)$ is $\varphi^t \colon W^* \to V^*$, where $\varphi^t(\ell) = \ell \circ \varphi$. Additionally,

- $\ker \varphi^t = \mathrm{Ann}(\mathrm{im}\, \varphi)$,
- $\mathrm{im}\, \varphi^t = \mathrm{Ann}(\ker \varphi)$ if $\dim V < \infty$,
- $\mathcal{M}(\varphi^t, \{f_j^*\}, \{e_i^*\} = \mathcal{M}(\varphi)^t$.

Definition 1.23
The **quotient vector space** for some subspace $U \subseteq V$ is given by $V/U = \{\text{cosets } v + U\}$. We have that

$$\begin{aligned} q \colon V &\longrightarrow V/U \\ v &\longmapsto v + U, \end{aligned}$$

is surjective with $\ker q = U$. This means the following diagram commutes, where any $\varphi \in \mathrm{Hom}(V, W)$ factors through V/U iff $U \subseteq \ker \varphi$.

$$\begin{tikzcd} V \arrow[rr, "\varphi"] \arrow[dr, "q"'] & & W \\ & V/U \arrow[ur, "\exists \overline{\varphi}"'] & \end{tikzcd}$$

1.3. Eigenspaces

The motivation for looking at invariant subspaces and eigenspaces is that they provide a concise way of determining the action of a linear operator, e.g. an operator in the set of endomorphisms $\mathrm{End}(V) = \mathrm{Hom}(V, V)$ of a vector space V. Note that vector spaces are special in how they can be characterized in such a way!

Definition 1.24
$W \subseteq V$ is an **invariant subspace** for $\varphi \in \operatorname{Hom}(V, W)$ if $\varphi(W) \subseteq W$.

Example 1.25
$\ker \varphi$, $\operatorname{im} \varphi$, eigenspaces $\ker(\varphi - \lambda I)$.

Theorem 1.26
If $V = \bigoplus V_i$, V_i invariant for φ, then there exists a basis where $\mathcal{M}(\varphi)$ is block diagonal, i.e. $\mathcal{M}(\varphi) = \begin{pmatrix} \varphi_{|V_1} & 0 \\ 0 & \varphi_{|V_2} \end{pmatrix}$

Corollary 1.27
*A basis of **eigenvectors** $v_i \in V$, $v_i \neq 0$, $\varphi(v_i) = \lambda_i v_i$ exists iff φ is **diagonalizable**, i.e.*

$$\mathcal{M}(\varphi, \{v_i\}) = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{pmatrix}.$$

Corollary 1.28
Eigenvectors of φ for distinct eigenvalues are linearly independent.

Theorem 1.29
If k is algebraically closed (e.g. $\mathbb{C}$), then any linear operator $\varphi \in \operatorname{Hom}(V, W)$ has an eigenvector.

Corollary 1.30
For any $\varphi \in \operatorname{Hom}(V, W)$ there exists a basis in which $\mathcal{M}(\varphi)$ is upper triangular. It holds that $\lambda \in k$ is an eigenvalue of φ iff $(\varphi - \lambda)$ is not invertible iff λ appears on the diagonal of a triangular matrix for φ.

Definition 1.31
We have the following notions:

- The **generalized kernel** is $\operatorname{gKer}(\varphi) = \ker(\varphi^N)$ for all N large, e.g. $\geq \dim V$.
- φ is **nilpotent** if $\varphi^N = 0$; $\ker \varphi \subseteq \ker \varphi^2 \subseteq \dots$, and there exists a basis s.t. $\mathcal{M}(\varphi)$ is block diagonal with blocks

$$\begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ * & & & 0 \end{pmatrix}.$$

- Generalized eigenspaces $V_\lambda = \mathrm{gKer}(\varphi - \lambda) = \ker(\varphi - \lambda)^N$ are linearly independent invariant subspaces.

Theorem 1.32
If k is algebraically closed then $V = \bigoplus V_\lambda$ of the generalized eigenspaces of φ. This gives the ***Jordan normal form****: $\mathcal{M}(\varphi)$ block diagonal with blocks of form*

$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ * & & & \lambda \end{pmatrix}.$$

Remark: φ is diagonalizable iff all blocks have size 1.

Definition 1.33
The **characteristic polynomial** of φ is $\chi_\varphi(x) = \det(xI - \varphi) = \prod_{\lambda_i}(x - \lambda_i)^{n_i}$, where $n_i = \mathrm{mult}(\lambda_i) = \dim V_{\lambda_i}$.
The **minimal polynomial** is $\mu_\varphi(x) = \prod_{\lambda_i}(x - \lambda_i)^{m_i}$, $m_i = \min\{m \mid V_{\lambda_i} = \ker(\varphi - \lambda_i)^m\} =$ size of largest Jordan block in V_{λ_i}.

Theorem 1.34 (Cayley-Hamilton)
$p(\varphi) = 0$ iff $\mu_\varphi \mid p(x)$. In particular $\mu_\varphi \mid \chi_\varphi$.

Corollary 1.35
Every linear operator satisfies its own characteristic equation.
Remark: φ is diagonalizable iff $m_i = 1\,\forall i$.

Theorem 1.36
Over $\mathbb{R}$, $\varphi\colon V \to V$ need not have eigenvectors, but considering $V_\mathbb{C} = V \times V = \{v + iw \mid v, w \in V\}$ and $\varphi_\mathbb{C}\colon V_\mathbb{C} \to V_\mathbb{C}$, where $\varphi_\mathbb{C}(v + iw) = \varphi(v) + i\varphi(w)$, we have that any real operator has an invariant subspace of dimension 1 (i.e. an eigenvector) or dimension 2!

1.4. Category Theory

Brief digression into category theory: due to the fact that categories provide a framework for expressing very general correspondances between different flavors of mathematical structure!

Definition 1.37
Categories have objects and morphisms $\mathrm{Mor}(A, B)$ for all $A, B \in \mathrm{ob}\,\mathcal{C}$, with operation given by composition. They obey the following axioms:

- $\forall A \in \mathrm{ob}\,\mathcal{C}$, $\exists\, \mathrm{id}_A \in \mathrm{Mor}(A, A)$ s.t. $f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$,

- $(f \circ g) \circ h = f \circ (g \circ h)$ (associativity).

Example 1.38
Sets, groups, vector spaces over k, topological spaces, and more!

Definition 1.39
A (covariant) **functor** $F\colon \mathcal{C} \to \mathcal{D}$ assigns

- to each $X \in \text{ob}\ \mathcal{C}$, $F(X) \in \text{ob}\ \mathcal{D}$,
- to $f \in \text{Mor}_{\mathcal{C}}(X, Y)$, $F(f) \in \text{Mor}_{\mathcal{D}}(F(X), F(Y))$,

such that $F(\text{id}_X) = \text{id}_{F(X)}$ and $F(g \circ f) = F(g) \circ F(f)$.
Contravariant functors reverse the direction of morphisms and the associated axiom.

Theorem 1.40
There is a natural transformation t between functors $F, G\colon \mathcal{C} \to \mathcal{D}$ given by taking for each $X \in ob\ \mathcal{C}$, $t_X \in \text{Mor}_{\mathcal{D}}(F(X), G(X))$ s.t.

$$\begin{tikzcd} X \arrow[d, "\forall f"'] & F(X) \arrow[r, "t_X"] \arrow[d, "F(f)"'] & G(X) \arrow[d, "G(f)"] \\ Y & F(Y) \arrow[r, "t_Y"] & G(Y) \end{tikzcd} \textit{ commutes.}$$

1.5. Bilinear Forms

Definition 1.41
A **bilinear form** on V is $b\colon V \times V \to k$, with linearity in each input, i.e.

- $b(u + v, w) = b(u, w) + b(v, w)$,
- $b(u, v + w) = b(u, v) + b(u, w)$,
- $b(\lambda u, v) = b(u, \lambda v) = \lambda b(u, v)$.

b is **symmetric** if $b(u, v) = b(v, u)$, and **skew-symmetric** if $b(u, v) = -b(v, u)$.

Theorem 1.42
There is a natural isomorphism given by

$$B(V) = \{\textit{bilinear } b\colon V \times V \to k\} \longrightarrow \text{Hom}(V, V^*)$$
$$b \longmapsto \varphi_b\colon v \to (b(v, \cdot)\colon V \to k)\,.$$

Then, $\operatorname{rank} b = \operatorname{rank} \varphi_b$*, and* b *is* ***nondegenerate*** *if* $\varphi_b \colon V \to V^*$ *is an isomorphism.*

Fact
In a basis $\{e_i\}$ of V, b is represented by a matrix $B = (b_{ij}) = (b(e_i, e_j))$. If $u = \sum x_i e_i$, $v = \sum y_i e_i$ are represented by column vectors X, Y, then $b(u, v) = X^t BY$.

Definition 1.43
The **orthogonal complement** of $S \subseteq V$ for b is $S^\perp = \{v \in V \mid b(v, w) = 0 \, \forall w \in S\} = \ker(v \mapsto \varphi_b(v)_{|S} \colon V \to S^*)$.

Theorem 1.44

- *If* b *is nondegenerate, then* $\dim S^\perp = \dim V - \dim S$.
- *If* b *is an inner product then* $S \cap S^\perp = \{0\}$ *and* $V = S \oplus S^\perp$.

Definition 1.45
A real **inner product** $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ is a **symmetric** **positive definite** bilinear form. Here, positive definite means $\langle u, u \rangle = \|u\|^2 > 0 \, \forall u \neq 0$.

Theorem 1.46 (Cauchy-Schwarz)
$\langle u, v \rangle \leq \|u\| \, \|v\|$.

Definition 1.47
Over $\mathbb{C}$ we consider **Hermetian inner products** $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ which are

- sesquilinear, i.e. $\langle \lambda u, v \rangle = \overline{\lambda} \, \langle u, v \rangle$,
- Hermitian symmetric, i.e. $\langle v, u \rangle = \overline{\langle u, v \rangle}$,
- definite positive.

The induced map $V \to V^*$ by $\langle \cdot, \cdot \rangle$ is $\mathbb{C}$-antilinear: $\varphi(\lambda u) = \overline{\lambda} \varphi(u)$.

Theorem 1.48
Every finite dimensional inner product space (over $\mathbb{R}$ *or* $\mathbb{C}$*) has an* ***orthonormal basis****, i.e. a basis* $(e_1, \ldots, e_n)$ *such that* $\langle e_i, e_j \rangle = \delta_{ij}$*. (Can be exhibited via building by induction using Gram-Schmidt.)*

1.6. Spectral Theorem

Definition 1.49
Let V,$\langle \cdot, \cdot \rangle$ be an inner product space (over $\mathbb{R}$ or $\mathbb{C}$), and $T \colon V \to V$ a linear operator. The **adjoint** operator $T^* \colon V \to V$ satisfies $\langle u, Tv \rangle = \langle T^* u, v \rangle \, \forall u, v \in V$. It corresponds to the transpose of T via $V \xrightarrow{\varphi} V^*$; over $\mathbb{C}$, the complex conjugate of T^t.

Fact

In an orthonormal basis, $\mathcal{M}(T^*) = \mathcal{M}(T)^t$ (real case) or $\overline{\mathcal{M}(T)}^t$ (complex Hermitian case). In addition, $\ker T^* = (\operatorname{im} T)^\perp$ and vice versa.

Definition 1.50
$T: V \to V$ is **self-adjoint** if $T^* = T$.

Definition 1.51
T is **orthogonal** (**unitary** over $\mathbb{C}$) if $T^* = T^{-1}$, i.e. $\langle Tu, Tv\rangle = \langle u, v\rangle$ $\forall u, v \in V$. In other words, T maps orthonormal bases to orthonormal bases.

Remark: If $S \subseteq V$ is invariant under a self-adjoint/orthogonal/unitary operator, then so is $S^\perp$. This motivates the **spectral theorems** below.

Theorem 1.52
- *If $T: V \to V$ is self-adjoint, then T is diagonalizable with real eigenvalues, and can be diagonalized in an orthonormal basis.*
- *If $T: V \to V$ is orthogonal for a real inner product, then V is a direct sum of orthogonal invariant subspaces of $\dim 1$ or $\dim 2$, with T acting by ± 1 on the $1-\dim$ pieces and rotations on the $2-\dim$ pieces.*
- *If $T: V \to V$ is unitary for a Hermitian inner product, then T is diagonalizable in an orthonormal basis, with eigenvalues $|\lambda_i| = 1$.*

Besides inner products, one can also consider arbitrary nondegenerate symmetric bilinear forms (without assuming positivity); e.g. over $\mathbb{R}$ (resp. $\mathbb{C}$), $\exists$ orthogonal basis such that

$$b(e_i, e_j) = \begin{cases} \pm 1 & i = j \\ 0 & i \neq j \end{cases} \left(\text{ resp. } b(e_i, e_j) = \delta_{ij}\right),$$

or skew-symmetric bilinear forms.

1.7. Tensor Algebra

Note: oftentimes you'll hear of the "universal property of tensor products" – all this means is that the tensor product is unique and well-defined in some natural sense. This is a good intuition to have, but formalizing it and using it is... trickier.

Definition 1.53
The **tensor product** of two vector spaces V, W is a vector space $V \otimes W$ with a bilinear map

$$\begin{aligned} \pi: V \times W &\longrightarrow V \otimes W \\ (v, w) &\longmapsto v \otimes w \end{aligned}$$

such that bilinear maps $V \times W \xrightarrow{b} U$ correspond bijectively with linear maps $V \otimes W \xrightarrow{\varphi} U$, via $\varphi(v \otimes w) = b(v, w)$. In other words, the following diagram commutes:

$$\begin{tikzcd} V \times W \arrow[rr, "b"] \arrow[dr, "\pi"'] & & U \\ & V \otimes W \arrow[ur, dashed, "\exists!\,\phi"'] & \end{tikzcd}$$

Elements of $V \otimes W$ are finite linear combinations $\sum v_i \otimes w_i$. If $\{e_i\}$ of V and $\{f_j\}$ of W are bases thereof, then $\{e_i \otimes f_j\}$ is a basis of $V \otimes W$.

Example 1.54

$V^* \otimes W \cong \mathrm{Hom}(V, W)$ by mapping $\ell \otimes w \in V^* \otimes W$ to $(v \mapsto \ell(v)w) \in \mathrm{Hom}(V, W)$.

Definition 1.55

The **trace** of an operator is conventionally given as $\operatorname{tr}(T\colon V \to V) = \sum \lambda_i \in k$. It can also be defined as

$$\begin{aligned} \operatorname{tr}\colon \mathrm{Hom}(V, V) \cong V^* \otimes V &\longrightarrow k \\ \ell \otimes v &\longmapsto \ell(v). \end{aligned}$$

Definition 1.56

In a similar sense we have a correspondance

$$\text{multilinear maps } V_1 \times \ldots \times V_n \to U \leftrightarrow \text{ linear maps } V_1 \otimes \ldots \otimes V_n \to U.$$

Theorem 1.57

The ***tensor power*** $V^{\otimes n} = \underbrace{V \otimes \ldots \otimes V}_{n \text{ times}}$ *contains subspaces*

- $\mathrm{Sym}^n(V) =$ ***symmetric tensors*** *($\leftrightarrow$ symmetric multilinear maps) with* $v_{\sigma(1)} \ldots v_{\sigma(n)} = v_1 \ldots v_n$,
- $\wedge^n(V)$ ***exterior powers****, or* ***alternating tensors*** *with* $v_{\sigma(1)} \wedge \ldots \wedge v_{\sigma(n)} = (-1)^\sigma v_1 \ldots v_n$.

Theorem 1.58

If $\dim V = n$*, then* $\wedge^n V$ *has* $\dim 1$*; for* $T\colon V \to V$*,* $\wedge^n T\colon \wedge^n V \to \wedge^n V$ *is multiplication by a scalar, the* ***determinant*** $\det(T) \in k$.

1.8. Modules

Modules are a generalization of vector spaces – they'll technically show up again in representation theory.

Definition 1.59
A **module** over a ring R (unlike a field, (commutative) rings do not require the existence of multiplicative inverses) is a set M with two operations:

- addition, with $+\colon M \times M \to M$,
- scalar multiplication, with $\times\colon R \times M \to M$.

Theorem 1.60
Finitely generated modules need not have a basis; those which do are called ***free modules****.*

Theorem 1.61
There is a bijection between $\mathbb{Z}$-modules and abelian groups.

Lemma 1.62
Every finitely generated $\mathbb{Z}$-module M with generators $(e_1, \dots, e_n)$ is a quotient of $\mathbb{Z}^n$, with

$$\begin{aligned} \varphi\colon \mathbb{Z}^n &\twoheadrightarrow M \\ \{a_i\} &\mapsto \sum a_i e_i. \end{aligned}$$

Furthermore, $\ker\varphi \subseteq \mathbb{Z}^n$ *is a free module, i.e.* $\exists T\colon \mathbb{Z}^m \to \mathbb{Z}^n$ *such that* $M \cong \mathbb{Z}^n / \operatorname{im} T$.

This next theorem is an amazing application of integer linear algebra!

Theorem 1.63
Every finitely generated abelian group is $\cong \mathbb{Z}^r \times \mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_k$ for integers $r, n_1, \dots, n_k$.

Corollary 1.64 (Classification Theorem for Finite Abelian Groups)
Every finite abelian group is $\cong \mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_k$ for integers $n_1, \dots, n_k$.

2 Group Theory

2.1. Basic Definitions

Definition 2.1
A **group** $(G, \cdot)$ is a set with an operation $\cdot\colon G \times G \to G$ such that the following laws hold:

- Identity: $\exists e \in G$ s.t. $\forall g \in G$, $eg = ge = g$,
- Inverse: $\forall g \in G$, $\exists g^{-1} \in G$ s.t. $gg^{-1} = e$,

- Associativity: $\forall a, b, c \in G$, $(ab)c = a(bc)$.

If G is commutative, i.e. $\forall g, h \in G\, gh = hg$, then it is **abelian**.

Example 2.2
$(\mathbb{Z}, +)$, $(\mathbb{Z}/n, +)$, $(\mathbb{C}^*, \cdot)$, symmetric group S_n; general linear group (of invertible matrices) $\mathrm{GL}_n(\mathbb{R})$, etc.; direct products $G \times H$, $\mathbb{Z}^n$.
Just like sets, groups can be finite ($\mathbb{Z}/n$, S_n, ...), countable ($\mathbb{Z}$, $\mathbb{Z}^n$, $\mathbb{Q}$, ...), or uncountable ($\mathbb{R}$, $\mathbb{C}$, ...).

Definition 2.3
$H \subseteq G$ is a subgroup if $e \in H$, $a \in H \implies a^{-1} \in H$, and $a, b \in H \implies ab \in H$.

Theorem 2.4 (Lagrange)
If $H \leq G$, then $|H| \mid |G|$. More specifically, $|G| = |H|[G\colon H]$, where $[G\colon H]$ is the number of cosets of H in G.

Example 2.5
If $H, H' \leq G$, then $H \cap H' \leq G$. Furthermore, all subgroups of $(\mathbb{Z}, +)$ are $\mathbb{Z}n = \{mn \mid m \in Z\}$ for some $n \geq 0$.

Definition 2.6
A **homomorphism** $\varphi\colon G \to H$ is a map such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. (Note this implies $\varphi(a)^{-1} = \varphi(a^{-1})$.) An **isomorphism** is a bijective homomorphism, and an **automorphism** is a bijective endomorphism. The set $(\mathrm{Aut}(G), \circ)$ itself is a group.

Definition 2.7
Given a homomorphism $\varphi\colon G \to H$, we define

- the **kernel** of φ: $\ker \varphi = \{g \in G \mid \varphi(g) = e_H\} \leq G$, where φ injective $\iff \ker \varphi = \{e\}$;
- the **image** of φ: $\operatorname{im} \varphi = \{\varphi(g) \mid g \in G\} \leq H$, where φ surjective $\iff \operatorname{im} \varphi = H$.

Definition 2.8
Given $a \in G$, define $\varphi\colon k \mapsto a^k\colon \mathbb{Z} \to G$, which is a homomorphism with $\operatorname{im} \varphi = \langle a \rangle$, the subgroup of G generated by a. As before, $\ker \varphi = \mathbb{Z}n$, where $n =$ the order of a, which is $\min\{n > 0 \text{ s.t. } a^n = e\}$. Thus, the **cyclic** group $\langle a \rangle$ is $\cong \mathbb{Z}/n$ if a has order n, $\cong \mathbb{Z}$ if infinite order. (Ergo, $a_1, \ldots, a_k$ generate G if every element of G is a product of a_i and their inverses).

An **equivalence relation** on a set A can be thought of as a set defined by a relation $\sim$ on A satisfying the following three axioms for all $a, b, c \in A$:

- reflexivity: $a \sim a$,

- symmetry: $a \sim b \iff b \sim a$,
- transitivity: $a \sim b, b \sim c \implies a \sim c$.

Theorem 2.9
A subgroup $H \leq G$ determines an equivalence relation given by $a \sim b$ iff $a^{-1}b \in H$, whose equivalence classes are the (left) ***cosets*** *$aH = \{ah \mid h \in H\}$. The* ***quotient set*** *G/H is the set of cosets aH. The index of H is $[G : H] = |G/H| = |G|/|H|$, if G is finite.*

Corollary 2.10
For finite G with $H \leq G$, we have

- $|H| \mid |G|$,
- $a \in G \implies |\langle a \rangle| \mid |G|$,
- $|G| = p$ *prime* $\implies G \cong \mathbb{Z}/p$.

Definition 2.11
A subgroup $H \leq G$ is **normal** iff $aH = Ha$ for all $a \in G$, which holds iff $aHa^{-1} = H$ for all $a \in G$.

Theorem 2.12
The operation $(aH) \cdot (bH) = abH$ makes G/H a group iff H is a normal subgroup.

Theorem 2.13
For all $\varphi \colon G \to H$, $\ker \varphi = K \trianglelefteq G$, and $\operatorname{im} \varphi = G/K$.
If φ is surjective, we have an ***exact sequence*** *$\{1\} \to K \hookrightarrow G \xrightarrow{\varphi} H \to \{1\}$, where $\operatorname{im} i = \ker \varphi$.*

Example 2.14
We have the following exact sequences for $H \trianglelefteq G$:

- $\{1\} \to H \hookrightarrow G \to G/H \to \{1\}$;
- $0 \to \mathbb{Z}/m \to \mathbb{Z}/mn \to \mathbb{Z}/n \to 0$ ($\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$ iff $\gcd(m, n) = 1$);
- $\{e\} \to \mathbb{Z}/3 \to S_3 \xrightarrow{\text{sign}} A_3 \cong \mathbb{Z}/2 \to \{e\}$.

Theorem 2.15
A homomorphism $G \xrightarrow{\varphi} H$ factors through $G \to G/K \xrightarrow{\overline{\varphi}} H$ iff $K \leq \ker \varphi$.

Definition 2.16
G is **simple** if its only normal subgroups are $\{e\}$ and itself.

Example 2.17
Some simple groups include $\mathbb{Z}/p$ for prime p and the alternating group A_n for $n \geq 5$.

Example 2.18
The **center** $Z(G) = \{z \in G \mid zg = gz \, \forall g \in G\}$ is a normal subgroup (abelian: $zz' = z'z$).

Example 2.19
The **commutator** subgroup $[G, G] = \{\prod_{\text{finite}} [a_i, b_i]\}$, where $[a, b] = aba^{-1}b^{-1}$, is normal, and $G/[G, G] = \text{Ab}(G)$ (abelianization) is the largest abelian quotient of G. Thus, for all $G \xrightarrow{\varphi} H$ with H abelian, φ factors $G \to \text{Ab}(G) \xrightarrow{\overline{\varphi}} H$.

2.2. Group Actions

Group actions allow us to talk about groups as encoding the symmetries of an object! This is where Burnside's lemma of combinatorics fame arises!

Definition 2.20
The **G-action** on a set S is a function $(g, s) \mapsto g \cdot s \colon G \times S \to S$ such that for all $s \in S$ and $g, h \in G$, we have $es = s$ and $(gh)s = g(hs)$. There is a bijective correspondence between actions defined as such and homomorphisms $\rho \colon G \to \text{Perm}(S)$. An action is **faithful** if ρ is injective; **transitive** if $\forall s, t \in S \; \exists g$ s.t. $gs = t$ (i.e. there is only 1 orbit).

Definition 2.21
The **orbit** of $s \in S$ is $\mathcal{O}_s = G \cdot s = \{g \cdot s \mid g \in G\}$. These form a partition of S as $S = \bigsqcup$ orbits.

Definition 2.22
The **stabilizer** of s is $\text{Stab}(s) = \{g \in G \mid g \cdot s = s\} \leq G$.

Theorem 2.23
Elements in the same orbit have conjugate stabilizer subgroups, i.e. $\text{Stab}(g \cdot s) = g \, \text{Stab} \, g^{-1} \leq G$.

Theorem 2.24 (Orbit-Stabilizer)
If $H = \text{Stab}(s)$, *then* $gH \mapsto g \cdot s$ *defines a bijection between* G/H *and* $\mathcal{O}_s$, *with* $|\mathcal{O}_s| \cdot |\text{Stab}(s)| = |G|$.

Lemma 2.25 (Burnside)
For G, S *finite, let* $S^g = \{s \in S \mid gs = s\}$ *be the fixed points of* $g \in G$. *Then,*

$$\#\ \textit{orbits} = \frac{1}{|G|} \sum_{g \in G} |S^g|.$$

Example 2.26
G acts on itself by left multiplication. This gives $G \hookrightarrow \mathrm{Perm}(G)$, hence every finite group is isomorphic to a subgroup of S_n, where $n = |G|$.

Theorem 2.27 (Class Equation)
*G acts on itself by **conjugation**: g acts by $h \mapsto ghg^{-1}$. Now, orbits are conjugacy classes, the stabilizer $\mathrm{Stab}(h) = \{g \in G \mid gh = hg\} = Z(h)$, the **centralizer** of h.*
Thus, we have that $|G| = \sum_{C \subset G} |C|$, where for each conj. class $|C_h| = \frac{|G|}{|Z(h)|}$ divides $|G|$.

Corollary 2.28
For p-groups ($|G| = p^k$), the class equation implies $|Z(G)| \geq p$ (the number of conj. classes of size 1). Thus, $|G| = p^2$, p prime implies G is abelian ($\cong \mathbb{Z}/p \times \mathbb{Z}/p$ or $\mathbb{Z}/p^2$).

Example 2.29
There are 5 isomorphism classes of groups of order 8: $\mathbb{Z}/8$, $\mathbb{Z}/4 \times \mathbb{Z}/2$, $(\mathbb{Z}/2)^3$, D_4, Q.

Example 2.30
Considering finite subgroups $G \leq SO(3)$, the group of all orthogonal transformations of $\mathbb{R}^3$ with determinant 1, and examining the action of G on the poles, we have $G \cong$ one of $\mathbb{Z}/n$, D_n (regular n-gon), A_4 (tetrahedron), S_4 (cube), A_5 (dodecahedron/icosahedron).

2.3. Symmetric Group

Theorem 2.31
*The **symmetric group** S_n is generated by transpositions (ij), in fact by $s_i = (i\, i+1)$.*

Theorem 2.32
For all permutations σ in S_n, there exists a unique decomposition of σ as a product of disjoint cycles $(a_1 \dots a_k)$. Moreover, two permutations $\sigma, \tau \in S_n$ are in the same conjugacy class iff they have the same cycle lengths.

Definition 2.33
The **alternating group** A_n is defined as $A_n = \ker(\mathrm{sign}\colon S_n \to \mathbb{Z}/2)$. Similarly, it can be viewed as the set {products of even # of transpositions}. A conjugacy class in S_n which consists of even permutations is either 1 or 2 conj. classes in A_n; it splits into 2 iff the centralizer $Z(\sigma) \subset A_n$ ($\iff$ cycle lengths of σ are odd and distinct).

Theorem 2.34
A_n is simple for $n \geq 5$ (A_4 isn't: $\{\mathrm{id}, (ij)(kl)\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ is normal in A_4 and S_4).

Remark: This is why there is no closed formula for the roots of a polynomial of degree ≥ 5! To learn why, dive into Galois theory...

2.4. Sylow Theorems

Theorem 2.35 (Sylow Theorems)
Let $|G| = p^e m$, $p \nmid m$. Then, a ***Sylow p-subgroup*** *of G is a subgroup of order p^e.*

- *$\forall p$ prime where $p \mid |G|$, G contains a Sylow p-subgroup. (Consequence: G contains an element of order p.)*
- *All Sylow p-subgroup of G are conjugates of each other, and every subgroup of order p^k ($k \leq e$) is contained in a Sylow subgroup.*
- *The number s_p of Sylow p-subgroups satisfies $s_p \equiv 1 \pmod p$, $s_p | m = \frac{|G|}{p^e}$.*

Definition 2.36
If G has subgroups $N, H \leq G$ such that $N \cap H = \{e\}$ (e.g. because $\gcd(|N|, |H|) = 1$), and $|G| = |N||H|$, then $\forall g \in G$ there is a unique $n \in N, h \in H$ such that $g = nh$.
Now, if $N, H \trianglelefteq G$, then $G \cong N \times H$. However, if $N \trianglelefteq G$ but not H, we have that G is isomorphic to a **semidirect product** $N \rtimes_\varphi H$, where $\varphi \colon H \to \mathrm{Aut}(N)$ is given by conjugation inside G. Thus, the group law is defined as $(n, h) \cdot (n', h') = (n\varphi(h)(n'), hh')$.

Theorem 2.37
Given $H \leq G$ (e.g. p-Sylow), the number of conjugate subgroups $gHg^{-1} \leq G$ (e.g. all p-Sylow subgroups) is $|G/N(H)|$, where $N(H)$ is the ***normalizer*** *of H. This means $N(H) = \left\{g \in G \mid gHg^{-1} = H\right\} \leq G$ is the largest subgroup of G such that $H \trianglelefteq G$.*

Example 2.38
We have the following classifications of finite groups as per Sylow's theorems:

- $|G| = 15$: Sylow subgroups of order 3 and 5 are normal ($s_3 = s_5 = 1$), so $G \cong \mathbb{Z}/3 \times \mathbb{Z}/5$.
- $|G| = 21$: $s_3 \in \{1, 7\}$ and $s_7 = 1$, so either $G \cong \mathbb{Z}/3 \times \mathbb{Z}/7$ or $\mathbb{Z}/7 \rtimes \mathbb{Z}/3$.
- $|G| = 12$: $s_2 \in \{1, 3\}$ and $s_3 \in \{1, 4\}$ and one is normal. This gives 5 isomorphism classes, $\mathbb{Z}/4 \times \mathbb{Z}/3$, $(\mathbb{Z}/2)^2 \times \mathbb{Z}/3$, A_4, D_6, $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$.

2.5. Free Groups

Definition 2.39
The **free group** on n generators is $F_n = \langle a_1, \ldots, a_n \rangle = \left\{ \text{all reduced words } a_{i_1}^{m_1} \ldots a_{i_k}^{m_k} \right\}$. Words in $a_i^{\pm 1}$ never simplify except $a_i a_i^{-1} = a_i^{-1} a_i = 1$.

Theorem 2.40
Any group G with n generators $g_1, \ldots, g_n$ is a quotient of F_n via $\varphi \colon a_i \mapsto g \colon F_n \twoheadrightarrow G$. G is ***finitely presented*** *if $\ker \varphi$ is generated by a finite set $r_1, \ldots, r_k$ and their conjugates. We write $G \cong \langle g_1, \ldots, g_n \mid r_1, \ldots, r_k \rangle = F_n / \langle \text{normal subgroup generated by conjugates of } r_j \rangle$.*

Definition 2.41
The **Cayley graph** of G with generators g_i: vertices are elements of G and edges connect g to gg_i for all $g \in G$ and all g_i.

Definition 2.42
A **normal form** for elements of $G = \langle g_1, \ldots, g_n \mid r_1, \ldots, r_k \rangle$ is a set of words in $g_1^{\pm 1} \ldots g_n^{\pm 1}$ such that every element of G appears exactly once among those words.

Example 2.43
Some examples of groups and their generators:

- $S_n \cong \left\langle s_1, \ldots, s_{n-1} \mid s_i^2 = 1,\ s_i s_j = s_j s_i\ \forall |i,j| \geq 2,\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \right\rangle$.
- $\mathrm{SL}_2(\mathbb{Z})$ is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
- $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) / \{\pm I\} = \left\langle S, T \mid S^2, (ST)^3 \right\rangle$

3 Representation Theory

3.1. Basic Definitions

Definition 3.1
A **representation** of G is a vector space V on which G acts by linear operators, i.e. $\rho \colon G \to \mathrm{GL}(V)$ is a homomorphism.
A **subrepresentation** is a subspace $W \subseteq V$ invariant under G, with $\forall g \in G\ g(W) = W$. V is **irreducible** if it has no nontrivial subrepresentations.

Theorem 3.2
For finite G and finite dimensional V over $\mathbb{C}$: every $g\colon V \to V$ has finite order, and $g^n = \mathrm{id} \implies$ diagonalizable, with $\lambda_j = e^{2\pi i k/n}$.

Theorem 3.3
If G is abelian, all operators $g\colon V \to V$ are simultaneously diagonalizable, and so irreducible representations are 1-dimensional. These correspond to elements of the dual group $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$. (Note that $\widehat{\mathbb{Z}/m} \cong \mathbb{Z}/m$.)

Definition 3.4
A **homomorphism** of representations is a G-**equivariant** linear map, i.e. $\varphi(gv) = g\varphi(v)$.

Theorem 3.5
Let V, W be representations of G. Then the following are representations of G as well:

- $V \oplus W$;
- $V \otimes W$ $(g\colon v \otimes w \mapsto gv \otimes gw)$;
- V^* $(\ell \mapsto \ell \circ g^{-1})$;
- $V^* \otimes W \cong \mathrm{Hom}(V, W)$ $(\varphi \mapsto g \circ \varphi \circ g^{-1})$.

With respect to the final case, note that the invariant subspace $\mathrm{Hom}(V, W)^G$, given by $\{\varphi \in \mathrm{Hom}(V, W) \mid g\varphi = \varphi \,\forall g \in G\}$ is equal to $\mathrm{Hom}_G(V, W)$.

Theorem 3.6
Any $\mathbb{C}$-representation of a finite group G admits an invariant Hermitian inner product, with respect to which G acts by unitary operators.

Theorem 3.7
If V is a representation of a finite group (over $\mathbb{C}$), then for any $W \subseteq V$ invariant subspace there exists some $U \subseteq V$ invariant subspace such that $V = U \oplus W$. Thus any $\mathbb{C}$-representation of a finite group decomposes into a direct sum of irreducibles.

Lemma 3.8 (Schur)
Let V, W be irreducible representations of G.

- *Any homomorphism $\varphi \in \mathrm{Hom}_G(V, W)$ is either 0 or an isomorphism;*
- *All isomorphisms of an irreducible representation are multiples of* id: $\mathrm{Hom}_G(V, V) = \mathbb{C} \cdot \mathrm{id}_V$.

Example 3.9
Some representations of S_n:

- trivial representation $U = \mathbb{C}$, σ acts by id;
- alternating representation $U' = \mathbb{C}$, σ acts by $(-1)^\sigma$;
- standard representation ($\dim n-1$) $V = \{z_1, \ldots, z_n \mid \sum z_i = 0\} \subset \mathbb{C}^n$, σ acts by permuting coordinates: $e_i \mapsto e_{\sigma(i)}$.

U, U', V are the only irreducible representations of S_3.

3.2. Characters

Characters enable us to encapsulate all the information about the eigenvalues of a conjugacy class of group elements, viewed as linear operators. Thus, they simplify many of the otherwise tedious arguments in breaking down finite representations into invariant ones.

Theorem 3.10
Let G be a group and V a representation thereof. The ***character*** *is a function $\chi_V : G \to \mathbb{C}$, with $\chi_V(g) = \operatorname{tr}(g : V \to V)$.*

Remark: In terms of eigenvalues, $\operatorname{tr}(g) = \sum \lambda_i$, and $\operatorname{tr}(g^k) = \sum \lambda_i^k$, so χ_V recovers all symmetric polynomial expressions in $\{\lambda_i\}$.

Fact
$\chi_V : G \to \mathbb{C}$ is a class function (invariant on conjugacy classes), i.e. $\chi_V(hgh^{-1}) = \chi_V(g)$.

Theorem 3.11
Let V, W be representations of G. Then, we have that

- $\chi_{V \oplus W} = \chi_V + \chi_W$;
- $\chi_{V \otimes W} = \chi_V \cdot \chi_W$;
- $\chi_{V^*} = \overline{\chi_V}$;
- $\chi_{\operatorname{Hom}(V,W)} = \overline{\chi_V} \chi_W$.

Fact
For a permutation representation, in which G acting on S corresponds to G acting on V with basis $\{e_s\}_{s \in S}$, with $g \cdot e_s = e_{g \cdot s}$, we have that

$$\chi(g) = \#\{s \in S \mid g \cdot s = s\} = |S^g|.$$

Definition 3.12
The **character table** of G lists, for each irreducible representation V_i, the value of χ_{V_i} on each conjugacy class.

Example 3.13
The character table of D_4 is

	1	1	2	2	2
D_4	1	r^2	r	s	sr
χ_1	1	1	1	1	1
χ_2	1	1	−1	1	−1
χ_3	1	1	1	−1	−1
χ_4	1	1	−1	−1	1
χ_V	2	−2	0	0	0
χ_R	8	0	0	0	0

.

Theorem 3.14
Define

$$\varphi = \frac{1}{|G|}\sum_{g\in G} g\colon V \to V$$

as the projection from V onto $V^G = \{v \in V \mid gv = v\,\forall g\}$, so $\dim V^G = \operatorname{tr}\varphi = \frac{1}{|G|}\sum_g \chi_V(g)$.

Theorem 3.15
Let

$$H(\alpha,\beta) = \frac{1}{|G|}\sum_{g\in G}\overline{\alpha(g)}\beta(g)$$

be a Hermitian inner product on $\mathbb{C}_{class}(G)$, the space of class functions $G \to \mathbb{C}$. Then $\dim \operatorname{Hom}_G(V,W) = H(\chi_V,\chi_W)$.

Theorem 3.16
*The characters of irreducible representations of G form an **orthonormal basis** of $(\mathbb{C}_{class}(G), H)$. In particular, the number of irreducible representations is equal to the number of conjugacy classes.*

Theorem 3.17
The multiplicities a_i in the decomposition of a G-representation $W \cong \bigoplus_i V_i^{\oplus a_i}$ are given by $a_i = \dim \operatorname{Hom}_G(V_i, W) = H(\chi_{V_i}\chi_W)$. Moreover, $H(\chi_W,\chi_W) = \sum a_i^2$.

Corollary 3.18
The regular representation of G (the permutation representation for G acting on itself by left multiplication) contains each irreducible representation V_i with multiplicity $= \dim V_i$; therefore $|G| = \sum_i (\dim V_i)^2$.

Fact

These results allow us to construct character tables of various groups (e.g. S_4, A_4, S_5, A_5, $\ldots$) by starting from known representations, considering tensor products, and using $H(\cdot, \cdot)$ pairings and orthogonality to find irreducible pieces and the missing irreducible representations.