Algebra Cheatsheet
Owen Fuller

Vector Spaces

Field: A set with functions

$$\text{addition} = + : F \times F \to F; (\lambda, \mu) \mapsto \lambda + \mu$$

$$\text{multiplication} = . : F \times F \to F; (\lambda, \mu) \mapsto \lambda\mu$$

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

$$\lambda(\mu + \nu) = \lambda\mu + \lambda\nu \in F$$

for any $\lambda, \mu, \nu \in F$. The neutral elements are called $0_F, 1_F$. For all $\lambda, \mu \in F$

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

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

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

For every $\lambda \neq 0 \in F \exists \lambda^{-1} \neq 0 \in F$ such that:

$$\lambda(\lambda^{-1}) = 1_F \in F$$

Vector Space: over a field F is a pair consisting of an abelian group $V = (V, \dot{+})$ and a mapping

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

such that for all $\lambda, \mu \in F$ and $\vec{v}\,, \vec{w}\, \in V$ the following hold:

$$\lambda(\vec{v}\dot{+}\vec{w}) = (\lambda\vec{v})\dot{+}(\lambda\vec{w})$$
$$(\lambda + \mu)\vec{v} = (\lambda\vec{v})\dot{+}(\mu\vec{v})$$
$$\lambda(\mu\vec{v}) = (\lambda\mu)\vec{v}$$
$$1_F\vec{v} = \vec{v}$$

Basis of a Vector Space: A linearly independent generating set in V.
Fundamental Estimate of Linear Algebra: No linearly independent subset of a given vector space has more elements than a generating set. Thus if V is a vector space, $L \subset V$ a linearly independent subset and $E \subseteq V$ a generating set then:

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

Vector Subspace: A subset U of a vector space V is a vector subspace if U contains the zero vector, and whenever $u, v \in U$ and $\lambda \in F$ we have $u + v \in U$ and $\lambda u \in U$.

Linear Mappings

Linear Map: Let V, W be vector spaces over a field F. A mapping $f : V \to W$ is called linear (or a homomorphism of F-vector spaces) if for all $\vec{v}_1, \vec{v}_2 \in V$ and $\lambda \in F$ we have:

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

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

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

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

Rank-Nullity Theorem

Image: of linear mapping $f : V \to W$ is the subset: $\text{im}(f) = f(V) \subseteq W$. It is a vector subspace of W.
Kernel: or preimage of the zero vector of a linear mapping $f : V \to W$ is denoted by $\ker(f) := f^{-1}(0) = \{v \in V : f(v) = 0\}$. It is a subspace of V.
Rank-Nullity Theorem: Let $f : V \to W$ be a linear mapping between vector spaces. Then:

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

Dimension Theorem Let V be a vector space, and $U, W \subseteq V$ vector subspaces, then:

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

Rings

Ring Definition: A set with two operations $(R, +, \cdot)$ that satisfy:

- $(R, +)$ is an abelian group
- $(R, \cdot)$ is associative and that there is an identity element $1 = 1_R \in R$, with $1 \cdot a = a \cdot 1 = a$ for all $a \in R$
- The distributive laws hold (bracket multiplication)

Field: A non-zero, commutative ring F in which every non-zero element $a \in F$ has an inverse $a^{-1} \in F$, s.t $a \cdot a^{-1} = a^{-1} \cdot a = 1$
Proposition 3.1.11: The commutative ring $\mathbb{Z}/m\mathbb{Z}$ is a field iff m is prime.
Unit: Let R be a ring. An element $a \in R$ is a unit if it is invertible in R. $R^\times$ is the group of units of R.
Integral Domain: An integral Domain is a non-zero commutative ring that has no zero-devisors. So these properties hold:

- $ab = 0 \implies a = 0$ or $b = 0$
- $a \neq 0$ and $b \neq 0 \implies ab \neq 0$

Cancellation Law for Integral Domains: Let R be an integral domain and let $a, b, c \in R$. If $ab = ac$ and $a \neq 0$ then $b = c$.
Proposition 3.2.17: The commutative ring $\mathbb{Z}/m\mathbb{Z}$ is an integral domain iff m is prime.

Polynomials

The set of all polynomials over a ring R is denoted $R[X]$. $R[X]$ is a ring called: *the ring of polynomials with coefficients in R*. The zero and identity of $R[X]$ are the zero and identity of R respectively. **Lemma 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]

Algebraically Closed: A field F is algebraically closed If each non-constant polynomial $P \in F[X]\backslash F$ with coefficients in our field has has a root in our field F.

Subrings, Homomorphisms

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

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

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

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

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

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

Principal Ideal: Let R be a commutative ring. An ideal I of R is a principal ideal if $I = \langle t\rangle$ for some $t \in R$. i.e an ideal that is generated by a single element in R through multiplication.
Prop 3.4.18: Let R and S be rings and $f : R \to S$ a ring homomorphism. Then $\ker f$ is an ideal of R

Example: The ideals of $\mathbb{Z}$ are the principal ideals $m\mathbb{Z} \subseteq \mathbb{Z}$ for $m \geqslant 0$
Subring Test: Let R' be a subset of a ring R. Then R' is a subring iff

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

Def 3.4.23: A subset R' of R is a subring of R if R' itself is a ring under the operations of addition and multiplication defined in R.

Prop 3.4.29: Let $f : R \to S$ be a ring homomorphism.

- If R' is a subring of R then $f(R')$ is a subring of S. In particular, $\text{im} f$ is a subring of S.
- Assume $f(1_R) = 1_S$. Then if x is a unit in R, $f(x)$ is a unit in S and $(f(x))^{-1} = f(x^{-1})$

Equivalence Relations

A relation R on a set X is a subset $R \subseteq X \times X$. (Writing 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:

- **Reflexivity:** xRx
- **Symmetry:** $xRy \iff yRx$
- **Transitivity:** $(xRy$ and $yRz) \to xRz$

Well Defined: $g : (X/\sim) \to Z$ is well defined if i can find a mapping $f : X \to Z$ such that f has the property $x \sim y \to f(x) = f(y)$ and $g = \bar{f}$.

Factor Rings

Def 3.6.1: 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 with respect to I in R.
Def 3.6.3: Let R be a ring. Let $I \trianglelefteq R$ be an ideal. And let $\sim$ be defined by $x \sim y \iff x - y \in I$. Then the **factor ring of** R **by** I or **quotient of** R **by** I, is the set $(R/\sim)$ of cosets of I of R.
The Universal Property of Factor Rings: Let R be a ring and I an ideal of R.

- The mapping can: $R \to R/I$ sending r ro $r + I$ for all $r \in R$ is a surjective ring homomorphism with kernel I.
- If $f : R \to S$ is a ring homomorphism with $f(I) = \{0_S\}$, so that $I \subseteq \ker f$, then there is a unique ring homomorphism $\bar{f} : R/I \to S$ such that $f = \bar{f}\circ$ can

First Isomorphism Theorem for Rings: Let R and S be rings. Then every ring homomorphism $f : R \to S$ induces a ring homomorphism

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

Proof: Clearly $\bar{f}$ is surjective. Injective since $\ker f = \{0\}$, since the only element in the kernel of $\bar{f}$ is the coset $0 + \ker f$, the zero element of $R/\ker f$.

Modules

(Left) Module M**, over a ring** R (also known as an R-module) is a pair consisting of an abelian group $M = (M, \dot{+})$ and a mapping

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

Such that for all $r, s \in R$ and $a, b \in M$ the following holds:

- Distributive Laws
- Associativity Law
- $1_R a = a$

Test for a submodule: Let R be a ring and let M be an R-module. A subset M' of M is a submodule iff:

- $0_M \in M'$
- $a, b \in M' \implies a - b \in M'$
- $r \in R$, $a \in M' \implies ra \in M'$

Lemma 3.7.21(22): Let $f : M \to N$ be an R-homomorphism. Then $\ker f$ is a submodule of M and $\text{im} f$ is a submodule of N. And f is injective iff $\ker f = \{0_M\}$
Module Cosets: Let R be a ring, M an R-module and N a submodule of M. For each $a \in M$ the coset of a with respect to N in M is:

$$a + N = \{a + b : b \in N\}$$

Factor Modules: M/N is the factor of M by N, or the quotient of M by N, is the set $(M/\sim)$ of all cosets of N in M. The R-module M/N is the factor module of M by the submodule N.
Addition is defined as $(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N$
Scalar Multiplication is defined as $\lambda(m + N) = \lambda m + N$

Universal Property of Factor Modules: Let R be a ring, let L and M be R-modules, and N a submodule of M.

- The mapping can: $M \to M/N$ sending a to $a + N$ for all $a \in M$ is a surjective R-homomorphism with kernel N.
- If $f : M \to L$ is an R-homomorphism with $f(N) = \{0_L\}$, so that $N \subseteq \ker f$, then there is a unique homomorphism $\bar{f} : M/N \to L$ such that $f = \bar{f}\circ$can.

Determinants

Back to Basics

Permutations: The group of all permutations of the set $\{1, 2, ..., n\}$, also known as bijections from $\{1, 2, ..., n\}$ to itself, is denoted by $\mathcal{G}_n$ and is 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 others unchanged.
Inversion: An inversion of a permutation $\sigma \in \mathcal{G}_n$ is a pair (i, j) such that $1 \le i < j \le n$ and $\sigma(i) > \sigma(j)$.
Length: Is the number of inversions of the permutation σ. Written $\ell(\sigma)$. In formula we have $\ell(\sigma) = |\{(i, j) : i < j \text{ but } \sigma(i) > \sigma(j)\}|$
Sign: The sign of σ is the parity of the number of inversions of σ, i.e. $\text{sgn}(\sigma) = (-1)^{\ell(\sigma)}$. If the sign is $+1$ then it is an even permutation, if it is -1 it is odd. Also $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$.
Alternating Group: For $n \in \mathbb{N}$ the set of even permutations in $\mathcal{G}_n$ forms a subgroup of $\mathcal{G}_n$ because it is the kernel of the group homomorphism sgn: $\mathcal{G}_n \to \{+1, -1\}$. This is the alternating group A_n.

Determinants

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

$$A \mapsto \det(A) = \sum_{\sigma \in \mathcal{G}_n} \text{sgn}(\sigma) a_{1\sigma(1)} ... a_{n\sigma(n)}$$

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 satisfies:

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

It is symmetric if $U = V$ and $H(u, v) = H(v, u)$ for all $u, v \in U$.
Antisymmetric/alternating if $U = V$ and $H(u, u) = 0$ for all $u \in U$.

Multilinear Forms: Let $V_1, ..., V_n, W$ be F-vector spaces. A mapping $H : V_1 \times V_2 \times ... \times V_n \to W$ is a multilinear form if for each j the mapping $V_j \to W$ defined by $v_j \mapsto H(v_1, ..., v_j, ..., v_n)$ with the $v_i \in V_i$ arbitrary fixed vectors of V_i for $i \neq j$, is linear.
Alternating MLF: Let V and W be F-vector spaces. A multilinear form $H : V \times ... \times V \to W$ is alternating if it vanishes

on every n-tuple of elements of V that has at least two entries equal, i.e. if

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

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.

Rules for Determinants

Multiplicativity of the Determinant: Let R be a commutative ring and let $A, B \in \text{Mat}(n; R)$. Then

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

Determinantal Criterion for Invertibility: The determinant of a square matrix with entries in a field F is non-zero iff the matrix is invertible.
Consequences: If A is invertible then $\det(A^{-1}) = \det(A)^{-1}$, and if B is a square matrix then $\det(A^{-1}BA) = \det(B)$
Lemma 4.4.4: The determinant of a square matrix and of the transpose of the square matrix are equal, i.e. $\forall A \in$ Mat(n;R) with R a commutative ring:

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

Cofactors: Let $A \in \text{Mat}(n; R)$ for some commutative ring R, and i and j be integers 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.

Laplace's Expansion of the Determinant: 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:

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

Adjugate Matrix: Let $A \in \text{Mat}(n; R)$ for a commutative ring R. The adjugate matrix $\text{adj}(A)$ is the $(n \times n)$-matrix whose entries are $\text{adj}(A)_{ij} = C_{ji}$.
Cramer's Rule: Let A be an $(n \times n)$-matrix with entries in a commutative ring R. Then:

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

Invertibility of Matrices: A square matrix with entries in a commutative ring R is invertible iff its determinant is a unit in R. i.e. $A \in \text{Mat}(n; R)$ is invertible iff $\det(A) \in R^\times$
Eigenspace: For any $\lambda \in F$, the eigenspace of f with eigenvalue λ is:

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

Eigenvalues and Eigenvectors

Eigenval/vec: Let $f : V \rightarrow V$ be an endomorphism of an F-vector space V. A scalar $\lambda \in F$ is an eigenvalue of f iff there exists a non-zero vector $\vec{v} \in V$ such that $f(\vec{v}) = \lambda\vec{v}$ where $\vec{v}$ is the eigenvector.

Eigenspace: of f with eigenvalue λ is:

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

Existence of Eigenvalues: Each endomorphism of a non-zero finite dimensional vector space over an algebraically closed field has an eigenvalue.
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 $\det(A - xI_n) \in R[x]$ is called the characteristic polynomial, denoted by:

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

Characteristic Poly and Eigenvalues: 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

Special Matrices

Triangularisable: Let $f : V \rightarrow V$ be an endomorphism of a finite dimensional F-vector space V. When the characteristic polynomial $\chi_f(x)$ of f decomposes into linear factors in $F[x]$.
Diagonalisable: 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.
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.

Google

Markov Matrix: (or a stochastic matrix) is a matrix M whose entries are non-negative and such that the sum of the entries of each column equals 1.
Perron: if $M \in \text{Mat}(n; \mathbb{R})$ is a Markov matrix with positive entries, then the eigenspace $E(1, M)$ is one dimensional. i.e there exists a unique basis vector $\vec{v} \in E(1, M)$ all of whose entries are positive real numbers, $v_i > 0$ for all i, and such that the sum of it's entries are 1.

Inner Product Spaces

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 $\vec{x} = \vec{0}$

Inner Product: Let V be a vector space over $\mathbb{C}$. An inner product on V is a mapping

$$(-, -) : V \times V \rightarrow \mathbb{C}$$

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

- $(\lambda\vec{x} + \mu\vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})$
- $(\vec{x}, \vec{y}) = \overline{(\vec{y}, \vec{x})}$
- $(\vec{x}, \vec{x}) \geq 0$, with equality iff $\vec{x} = \vec{0}$

Length: In a real or complex inner product space the length or inner product norm $||\vec{v}|| \in \mathbb{R}$ of a vector is:

$$||\vec{v}|| = \sqrt{(\vec{v}, \vec{v})}$$

Orthogonal: Two vectors $\vec{v}, \vec{w}$ are orthogonal written $\vec{v} \perp \vec{w}$, iff $(\vec{v}, \vec{w}) = 0$.
Orthonomal Family: A family $(\vec{v}_i)_{i \in I}$ for vectors from an inner product space is an orthonormal family if all vectors $\vec{v}_i$ have length 1 and if they are pairwise orthogonal to each other, which means:

$$(\vec{v}_i, \vec{v}_j) = \delta_{ij}$$

An orthonormal family that is a basis is an orthonormal basis.

Orthogonal Complements and Projections

Orthorgonality: 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.
Proposition 5.2.2: 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: 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 mapping $\pi_U : V \to V$ that sends $v = p + r$ to p.
Cauchy-Schwarz inequality: Let $\vec{v}, \vec{w}$ be vectors in an inner product space. Then

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

With equality iff they are linearly dependent.
Proof: If $y = 0$, then it's true, so assume otherwise.
Let $z = x - \frac{(x,y)}{(y,y)}y$. Then $(z, y) = 0$. So $||x||^2 = ||z + \frac{(x,y)}{(y,y)}y||^2 = ||z||^2 + \frac{(x,y)^2}{(y,y)^2}||y||^2 = ||z||^2 + \frac{(x,y)^2}{||y||^2} \geq \frac{(x,y)^2}{||y||^2}$

$$x_1y_1 + \cdots + x_ny_n \leqslant \sqrt{x_1^2 + \cdots + x_n^2}\sqrt{y_1^2 + \cdots y_n^2}$$

The Norm: Satisfies:

- $||\vec{v}|| \geq 0$ with equality iff $\vec{v} = \vec{0}$
- $||\lambda\vec{v}|| = |\lambda| ||\vec{v}||$
- $||\vec{v} + \vec{w}|| \leq ||\vec{v}|| + ||\vec{w}||$, the triangle inequality

Gram-Schmidt Process: The Gram-Schmidt Formulae are:

$$\vec{w}_1 = \frac{\vec{v}_1}{\|\vec{v}_1\|}, \vec{w}_2 = \frac{\vec{v}_2 - (\vec{v}_2, \vec{w}_1)\,\vec{w}_1}{\|\vec{v}_2 - (\vec{v}_2, \vec{w}_1)\,\vec{w}_1\|}$$

Projection operator:

$$\text{proj}_{\mathbf{u}}(\mathbf{v}) = \frac{(\mathbf{u}, \mathbf{v})}{(\mathbf{u}, \mathbf{u})}\mathbf{u}$$

Gram-schmidt Process:

$$\mathbf{u}_1 = \mathbf{v}_1, \quad \mathbf{e}_1 = \frac{\mathbf{u}_1}{\|\mathbf{u}_1\|}$$

$$\mathbf{u}_2 = \mathbf{v}_2 - \text{proj}_{\mathbf{u}_1}(\mathbf{v}_2), \quad \mathbf{e}_2 = \frac{\mathbf{u}_2}{\|\mathbf{u}_2\|}$$

$$\mathbf{u}_3 = \mathbf{v}_3 - \text{proj}_{\mathbf{u}_1}(\mathbf{v}_3) - \text{proj}_{\mathbf{u}_2}(\mathbf{v}_3)$$

$$\mathbf{e}_3 = \frac{\mathbf{u}_3}{\|\mathbf{u}_3\|}$$

Adjoints and Self-Adjoints

Adjoint: Let V be an inner product space. Then two endomorphisms $T, S : V \to V$ are adjoint if for all $\vec{v}, \vec{w} \in V$:

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

In this case $S = T^*$ and we call S the *adjoint* of T. **Self-Adjoint:** An endomorphism of an inner product space $T : V \to V$ is self-adjoint if it equals its own adjoint, i.e if $T^* = T$.
Theorem: T^*T is self adjoint.
Proof: $((T^*T)x, y) = (y, T^*Tx) = (Ty, Tx) = (Tx, Ty) = (x, T^*Ty) \forall x, y \in V$ so $(T^*T)^* = T^*T$
Theorem: $\ker(T^*) = (\text{im}T)^{\perp}$
Proof: $x \in (\text{im}T)^{\perp} \iff \forall y \in \text{im}T \quad (y, x) = 0$
$\iff \forall v \in V \quad (Tv, x) = 0$
$\iff \forall v \in V \quad (v, T^*x) = 0$
$\iff T^*x = 0 \iff x \in \ker T^*$
Definition 5.3.7: Let $T : V \to V$ be a self-adjoint linear mapping on an inner product space V. Then: (1) Every eigenvalue of T is real. (relevant for $F = \mathbb{C}$
(2) If λ and μ are distinct eigenvalues of T with eigenvectors v, w, then $(v, w) = 0$
(3) T has an eigenvalue. (relevant for $F = \mathbb{R}$)

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

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

Where $\lambda_1, ..., \lambda_n$ are the (necessarily real) eigenvalues of A, repeated according to their multiplicity.
Spectral Theorem for Hermitian Matrices: Let A be a real $(n \times n)$-hermitian matrix. Then there is an $(n \times n)$-unitary matrix P such that:

$$\bar{P}^TAP = P^{-1}AP = \text{diag}(\lambda_1, ..., \lambda_n)$$

Where $\lambda_1, ..., \lambda_n$ are the (necessarily real) eigenvalues of A, repeated according to their multiplicity.
Hermitian Matrix: A complex square matrix such that $A = \bar{A}^T$

Jordan Normal Form

Nilpotent Jordan Block of size r: Define an $(r \times r)$-matrix $J(r)$, by the rule $J(r)_{ij} = 1$ for $j = i + 1$ and $J(r)_{ij} = 0$ otherwise. If $r = 1$ then we get a (1×1) zero matrix.
Jordan Block of size r and eigenvalue of λ: with $\lambda \in F$, with the rule

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

such that $DN = ND$
Theorem 6.2.2: Let F be an algebraically closed field. Let V be a finite dimensional vector space and let $\phi : V \to V$ be an endomorphism of V with characteristic polynomial:

$$\chi_{\phi}(x) = (\lambda_1 - x)^{a_1} (\lambda_2 - x)^{a_2} \ldots (\lambda_s - x)^{a_s}$$

$$\in F[x] \left(a_i \geqslant 1, \sum_{i=1}^{s} a_i = n\right)$$

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

$${}_{\mathcal{B}}[\phi]_{\mathcal{B}} = \text{diag}\left(J(r_{11}, \lambda_1), \ldots, J\left(r_{1m_1}, \lambda_1\right), J(r_{21}, \lambda_2), \ldots, J(r_{sm_s}, \lambda_s)\right)$$

With $r_{21}, ..., r_{1m_1}, r_{21}, ..., r_{sm_s} \geq 1$ such that:

$$a_i = r_{i1} + r_{i2} + \cdots + r_{im_i} (1 \leqslant i \leqslant s)$$

Lemma 6.3.1: There exists polynomials $Q_j(x) \in F[x]$ such that:

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

Definitions

Row Echelon Form:
-Leading entry in each row = 1
-Each leading entry is in a column to the right of the leading entry in the previous row
-Rows with all zeros below others
Reduced Row Echelon:
-Same as REF
-The leading entry in each row is the only non zero entry in it's column
Associative: $(a \times b) \times c = a \times (b \times c)$
Commutative: $a \times b = b \times a$
Distributive Law: $a \times (b + c) = a \times b + a \times c$
Monic Polynomial: When it's leading coefficient is 1
Monoid: Associative, closed and has an identity

Tranposition: A permutation that swaps two elements of the set and leaves all the others unchanged

Kronecker Delta: $\delta_{i,j} = \begin{cases} 1 & i=j \\ 0 & \text{otherwise} \end{cases}$ Injective: $\forall x, x' \in X, f(x) = f(x') \Rightarrow x = x'$

Surjective: $\forall y \in Y, \exists x \in X$ such that $y = f(x)$

Idempotent: If $f = f^2$

Counterclockwise Rotation Matrix: $\begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}$

Notation: let $a \in \mathbb{R}\backslash 0$ then let$[a] \in \{+1, -1\}$ be the sign of a.

Endomorphism: A morphism from something to itself. **Unitary Matrix:** Let $P \in \text{Mat}(m, \mathbb{C})$. P is uniatary if $\bar{P}^T P =$ identity. i.e $P^{-1} = \bar{P}^T$

Examples

- **Trace:** If two matrices have different traces, then they cannot represent the same endomorphism. Since the trace of a linear mapping is well defined, because $\text{tr}\left(P^{-1}MP\right) = \text{tr}(M)$ for any matrix M and invertible matrix P (i.e. a change of basis matrix P).
- **Symmetric bilinear form:** dot product on $\mathbb{R}^2$
- **Alternating bilinear form:** cross product on $\mathbb{R}^3$
- **Alternating MLF** on $V \times V$... n times: determinant of a real $n \times n$ matrix.
- f is injective iff $\ker = \{0\}$
- Non zero polynomial with more roots than degrees: $2(X^2 + X) \in \mathbb{Z}/4\mathbb{Z}$
- Ring where not every ideal is a principal ideal: $\mathbb{Z}[X]$
- An ideal in a ring that is not principal: $_{\mathbb{Z}[X]} < 2, X >$
- Commutative ring that is not an integral domain: $\mathbb{Z}/4\mathbb{Z}$
- Basis for $\mathbb{C}$: $(1, i)$.
- Inner Product on $\mathbb{C}$: $((z_1, w_1), (z_2, w_2)) = z_1\bar{z}_2 + w_1\overline{w}_2$
- Inner Product on $\mathbb{C}^2$: $((z_1, w_1), z_2, w_2)) = z_1\bar{z}_2 + w_1\bar{w}_2$
- Inner Product on $\mathbb{C}^3$: $\sum_{i=1}^3 x_i\bar{y}_i$
- A self-adjoint operator on $\mathbb{C}^3$ with respect to the inner product above: identity
- A non self-adjoint operator on $\mathbb{C}^3$ with respect to the inner product above: $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$
- Inner Product on $\mathbb{R}[X]$:
$$(P, Q) = \int_a^b P(X)Q(X)dX$$
- A non-zero symmetric bilinear form which is not an inner product: $((x_1, y_1), (x_2, y_2)) = x_1x_2$
- A non symmetric bilinear form on $\mathbb{R}^2$: $((x_1, y_1), (x_2, y_2)) = x_1y_2 - x_2y_1$
- Non-invertible matrix whose determinant is not zero: $2 \in \text{Mat}(1, \mathbb{Z})$
- Diagonalisable Matrix: $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$
- Non-Diagonalisable Matrix: $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$
- A matrix with entries in $\mathbb{C}$ which is a Jordan block of size 3 and eigenvalue not equal to 0 or 1: $\begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}$
- Invertible with trace=0: $\begin{bmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$
- No Eigenvalue Matrix: $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$
- A (3×3)-matrix all of whose entries are positive and real and that has exactly one eigenvalue equal to 1: $\frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$
- For a finite dimensional inner product space $(V, (-,-))$ and a subspace $U \subseteq V$ the orthogonal subspace to $U \subseteq V$ is:
$$U^{\perp} = \{\vec{v} \in V | (\vec{u}, \vec{v}) = 0 \text{ for all } \vec{u} \in U\} \subseteq V$$
The dimensions are:
$$\dim\left(U \cap U^{\perp}\right) = 0, \dim(U) + \dim\left(U^{\perp}\right) = \dim(V)$$