Linear Algebra 2 Notes

paraphrased by Tyler Wright

An important note, these notes are absolutely ***NOT*** *guaranteed to be correct, representative of the course, or rigorous. Any result of this is not the author's fault.*

1 Groups, Rings, and Fields

1.1 Definition of a Group

A group is a set G combined with a group operation $\circ : G \times G \to G$ such that:

- For all g, h, j in G, $g(hj) = (gh)j$ (associativity)
- There exists e in G such that $eg = ge = g$ for all g in G
- For all g in G, there exists g^{-1} in G such that $gg^{-1} = g^{-1}g = e$ where e is the identity of G.

1.2 Definition of a Homomorphism

A homomorphism between two groups G, H is a function $f : G \to H$ such that $f(gh) = f(g)f(h)$ for all g, h in G.

1.3 Properties of Homomorphisms

We can derive some properties of homomorphisms, for G, H groups, and $f : G \to H$ a homomorphism:

- The image of the identity in G is the identity in H
- The kernel of f is a subgroup of G
- The image of f is a subgroup of H
- Bijective homomorphisms are isomorphisms.

1.4 Definition of a Ring

A ring with unity is a set R along with an addition map $+$, and a multiplication map $\circ$ where $+, \circ : R \times R \to R$ such that:

- $(R, +)$ is an abelian group (of which the identity is called zero)
- The multiplication operation is associative
- The multiplication operation has a two-sided identity not equal to the zero identity (called one)
- For all a, b, c in R, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

A ring is commutative if the multiplication operation is commutative.

1.5 Definition of a Subring

For the ring $R = (R', +, \circ)$ and S a set, S is a subring of R if $S \subseteq R'$ and $(S, +, \circ)$ is a ring.

1.6 Definition of a Ring Homomorphism

For rings with unity R and S, $f : R \to S$ is a ring homomorphism if for all a, b in R:

$$
\begin{aligned}
f(a+b) &= f(a) + f(b) \\
f(ab) &= f(a)f(b) \\
f(1_R) &= 1_S
\end{aligned}
$$

Essentially, this says that f is a homomorphism for the groups formed by R and S under addition and multiplication.

1.7 Definition of a Field

A field $\mathbb{F}$ is a ring with unity with the following properties:

- $(\mathbb{F} \setminus \{0\}, \circ)$ is an abelian group.

1.8 Definition of the Field Characteristic

For a field $\mathbb{F}$, the field characteristic char($\mathbb{F}$) is the smallest positive integer n such that:

$$\sum_{i=1}^{n} 1 = 1 + 1 + \ldots + 1 = 0,$$

or zero if no such value n exists.

1.9 Definition of the Algebraic Closure of Fields

A field $\mathbb{F}$ is called algebraically closed if all non-constant polynomials with coefficients in $\mathbb{F}$ also has a root in $\mathbb{F}$.

2 Vector Spaces

2.1 Definition of a Vector Space

A vector space over a field $\mathbb{F}$ is a set V with an addition operation $+ : V \times V \to V$ and a scalar multiplication operations $\circ : \mathbb{F} \times V \to V$ such that for all a, b in $\mathbb{F}$ and v, w in V:

- $(V, +)$ is an abelian group
- $1 \circ v = v$ where 1 is the multiplicative identity of $\mathbb{F}$
- $(ab) \circ v = a \circ (b \circ v)$
- $(a + b) \circ v = a \circ v + b \circ v$
- $a \circ (v + w) = a \circ v + a \circ w$.

2.2 Definition of a Subspace

For V a vector space over the field $\mathbb{F}$ and W a set, W is a subspace of V if it is a subset of V and is a vector space with respect to the addition and scalar multiplication defined by V.

It is sufficient to verify that for any a in $\mathbb{F}$ and v, w in W we have that $a(v + w)$ is in W.

2.3 Definition of a Linear Combination

For a set V with addition operation $+$, a field $\mathbb{F}$ and n in $\mathbb{N}$, a linear combination of $v_1, \dots, v_n$ in V is:

$$\sum_{i=1}^{n} a_i v_i,$$

for $a_1, \dots, a_n$ in $\mathbb{F}$.

2.4 Definition of the Span

For a set V with addition operation $+$ and a field $\mathbb{F}$, the span of $W \subseteq V$ is the set of all the linear combinations of the values in W. Denoted by $\operatorname{span}(W)$.

2.5 Definition of Linear Independence

For a vector space V and $W \subseteq V$, we say W is linearly dependent if there exists a non-trivial linear combination of all the vectors in W equal to zero (and linearly independent otherwise).

2.6 Properties of Linear Independence

For a vector space V with $W \subseteq V$:

- $0 \in W \Rightarrow W$ is linearly independent
- W linearly independent $\Rightarrow$ any $X \subseteq W$ is linearly independent
- If there's a linearly dependent subset of W, then W is linearly dependent.

2.7 Definition of a Basis

For a vector space V with $W \subseteq V$, if W is linearly independent and $\text{span}(W) = V$, we say that W is a basis of V.

Saying W is a basis is equivalent to saying that each vector in V can be **uniquely** written as a linear combination of vectors in W.

Additionally, for finite vector spaces, we have that all bases have the same amount of elements.

2.8 Definition of Dimension

For non-infinite bases, we say that the value of the basis is the dimension of the vector space it is a member of. Vector spaces with such bases are called finite-dimensional and all other vector spaces are infinite-dimensional.

By convention, for a vector space V, $\dim(\{0_V\}) = 0$.

2.9 Isomorphisms from Dimension

For V, W finite-dimensional vector spaces over $\mathbb{F}$ with $\dim(V) = \dim(W)$, then $V \cong W$.

If we set $n = \dim(V)$, we have that $V \cong \mathbb{F}^n$.

Such an isomorphism can be found by mapping a vector in terms of some chosen basis vectors ($v = a_1v_1 + a_2v_2 + \cdots + a_nv_n$) to the coefficients $(a_1, a_2, \ldots, a_n)$.

3 Linear Maps

3.1 Definition of a Linear Map

Let V, W be vector spaces over a field $\mathbb{F}$, we have that $f : V \to W$ is a linear map if for all a, b in $\mathbb{F}$ and u, v in V:

$$f(au + bv) = af(u) + bf(v).$$

A bijective linear map is called an isomorphism. If $f : V \to W$ is an isomorphism, we say that V and W are isomorphic, denoted by $V \cong W$.

3.2 The Kernel of Linear Maps

Let V, W be vector spaces over a field $\mathbb{F}$, and $f : V \to W$ be a linear map. We define the kernel of f as:

$$\mathrm{Ker}(f) := \{v \in V : f(v) = 0_{\mathbb{F}}\}.$$

Saying $\mathrm{Ker}(f)$ is $\{0_{\mathbb{F}}\}$ is equivalent to saying f is injective.

3.3 The Image of Linear Maps

Let V, W be vector spaces over a field $\mathbb{F}$, and $f : V \to W$ be a linear map. We define the image of f as:

$$\mathrm{Im}(f) := \{w \in W : \exists\, v \in V \text{ with } f(v) = w\}.$$

Saying $\mathrm{Im}(f)$ is W is equivalent to saying f is surjective.

3.4 The Inverse of Linear Maps

For a bijective linear map f, the inverse of f is also linear.

3.5 Properties of the Set of Linear Maps

For V, W vector spaces over a field $\mathbb{F}$, we define $\mathcal{L}(V, W)$ to be the set of all linear maps from V to W.

3.6 The Rank-Nullity Theorem

For V, W finite-dimensional vector spaces and $f : V \to W$ a linear map, we have that:

$$\dim(V) = \dim(\mathrm{Ker}(f)) + \dim(\mathrm{Im}(f)).$$

Thus, for a linear map $f : V \to V$, if f is injective or surjective then it's an isomorphism.

4 Matrices

4.1 Definition of a Matrix

For m, n in $\mathbb{Z}_{>0}$ and $\mathbb{F}$ a field. An $m \times n$ matrix with entries in $\mathbb{F}$ is a map $M : [m] \times [n] \to \mathbb{F}$, more commonly written as $M = (a_{ij})$ representing the rectangular array of values held by M.

The set of all $m \times n$ matrices over $\mathbb{F}$ is denoted by $M_{m \times n}(\mathbb{F})$.

4.2 Types of Matrix

For m, n in $\mathbb{Z}_{>0}$ and $\mathbb{F}$ a field, let M be in $M_{m \times n}(\mathbb{F})$. We have the following types of matrix:

- **Square**: where $m = n$
- **Upper Triangular**: if $a_{ij} = 0$ for $i > j$
- **Lower Triangular**: if $a_{ij} = 0$ for $i < j$
- **Diagonal**: if $a_{ij} = 0$ for $i \neq j$
- **Symmetric**: if $a_{ij} = a_{ji}$
- **Anti-symmetric**: if $a_{ij} = -a_{ji}$.

4.3 Properties of the Space of Matrices

For m, n in $\mathbb{Z}_{>0}$ and $\mathbb{F}$ a field, we have that $M_{m\times n}(\mathbb{F})$ is a vector space over $\mathbb{F}$ where matrices are added and multiplied by scalars component-wise. So, for
$M_1 = (a_{ij}), M_2 = (b_{ij})$ in $M_{m\times n}$ and c in $\mathbb{F}$ we have:

$$cM_1 = (ca_{ij})$$
$$M_1 + M_2 = (a_{ij} + b_{ij}).$$

Additionally, the zero vector is $M_0 = (0)$ and the vector space has a basis consisting of M_{ij} where all entries are zero except the $(i, j)^{\text{th}}$ entry. This leads to the conclusion that the dimension is mn and thus that $M_{m\times n} \cong \mathbb{F}^{mn}$.

4.4 Matrix Multiplication

For a, b, c in $\mathbb{Z}_{>0}$ and a field $\mathbb{F}$, we can define the multiplication of the two matrices $X = (x_{ij})$ in $M_{a\times b}$ and $Y = (y_{ij})$ in $M_{b\times c}$ as follows:

$$XY := (\sum_{k=1}^{b} x_{ik}y_{kj}).$$

This operation is not commutative in general but is associative.

For A, B in M_n, we have that AB is also in M_n. This, along with matrix addition, makes M_n a ring with unity with multiplicative identity $I_n := (\delta_{ij})$. However, there exists A, B in M_n such that $AB = 0$ so, M_n is not a field.

4.5 Matrices of Linear Maps

For V, W vector spaces over a field $\mathbb{F}$, for some m, n in $\mathbb{Z}_{>0}$ we have $A = \{v_1, \ldots, v_n\}$, $B = \{w_1, \ldots, w_n\}$ bases for V and W respectively. Given f in $\mathcal{L}(V, W)$, the matrix associated to f (with respect to the bases A and B) is the $m \times n$ matrix:

$$M_{BA}(f) = (a_{ij}),$$

where we define a_{ij} by:

$$f(v_j) = \sum_{i=1}^{m} a_{ij}w_i,$$

for each j in $[n]$.

4.6 Matrices of Composed Linear Maps

For U, V, W vector spaces over a field $\mathbb{F}$, for some l, m, n in $\mathbb{Z}_{>0}$ we have $A = \{u_1, \ldots, u_n\}$, $B = \{v_1, \ldots, v_n\}$, $C = \{w_1, \ldots, w_n\}$ bases for U, V, W respectively. Given g, f in $\mathcal{L}(V, W)$, we have:

$$M_{CA}(g \circ f) = M_{CB}(g)M_{BA}(f).$$

4.7 Transition Matrices

For a finite-dimensional vector space V, with an identity I and bases A, A', we call $M_{A'A}(I) = C_{A'A}$ a transition matrix.

We have that $C_{A'A}$ is invertible and $C^{-1}_{A'A} = C_{AA'}$.

Essentially, the transition matrix transforms between bases.

4.8 Matrix Transitions

For a finite-dimensional vector space V, with $f : V \to V$ a linear operator, and bases A, B:

$$\begin{aligned} M_{BB}(f) &= C^{-1}_{AB}M_{AA}(f)C_{AB} \\ &= C_{BA}M_{AA}(f)C_{AB}. \end{aligned}$$

4.9 Similar Matrices

For matrices A', A, we say that A' and A are similar if there exists an invertible matrix C such that:

$$A' = C^{-1}AC.$$

This is denoted by $A' \sim A$. Similarity forms an equivalence relation on the space of square matrices.

If we have $A \sim A'$ and A represents some linear operator f for some basis B, then we have that for some basis B', f has matrix A'.

5 Eigenvectors and Eigenvalues

5.1 Definition of an Eigenvectors and Eigenvalues

For a vector space V over $\mathbb{F}$ with $f : V \to V$ a linear operator, a non-zero vector v in V is an eigenvector if $f(v) = \lambda v$ for some λ in $\mathbb{F}$ which is called the eigenvalue corresponding to v.

5.2 Definition of an Eigenspace

For a vector space V over $\mathbb{F}$ with $f : V \to V$ a linear operator and some eigenvalue λ, we define the eigenspace of λ as the set of eigenvectors with eigenvalue λ.

This is denoted by $E(\lambda)$ and $E(\lambda) \cup \{0_V\}$ forms a subspace of V. The dimension of $E(\lambda)$ is the geometric multiplicity of λ.

6 Direct Sums and Projections

6.1 Definition of a Direct Sum

For V, W vector spaces, we define the direct product of V and W as:

$$V \oplus W := \{(v, w) : v \in V, w \in W\},$$

with addition and scalar multiplication defined coordinate-wise and zero vector $(0_V, 0_W)$.

6.2 The Equivalence of Direct Sums

For $V, W \subseteq U$, we have that the following are equivalent:

- $U = V \oplus W$
- Each element in U can be written uniquely as the sum of elements in V and W
- The map $f : V \oplus W \to U; (v, w) \mapsto v + w$ is isomorphism.

6.3 The Addition Map for Direct Sums

For V, W subspaces of a vector space U, and $f : V \oplus W \to U$ defined by:

$$f((v, w)) = v + w,$$

we have that:

- f is linear
- f is injective if and only if $V \cap W = \{0\}$
- f is surjective if and only if $V \cup W$ spans U.

6.4 Projections

For V, W subspaces of U with $U = V \oplus W$, the projection **onto** V along W is the linear operator $P_{V,W} : U \to U$ where:

$$P_{V,W}(u) = v,$$

where $u = v + w$ for some unique v in V and w in W.

We have that for a linear operator P, P is a projection if and only if $P \circ P = P$.

6.5 f-invariance

For a vector space V with $U \subseteq V$ a subspace and $f : U \to U$ a linear operator, we have that U is f-invariant if for all u in U we have $f(u)$ in U.

The eigenspaces of f are examples of f-invariant spaces.

6.6 Matrices of Linear Maps (using f-invariance)

For $U, W \subseteq V$ subspaces of the vector space V such that $V = U \oplus W$, let B_U, B_W be finite bases of U and V respectively. If we have a linear operator $f : V \to V$ such that U and W are f-invariant, we have that the matrix with respect to the basis $B = B_U \cup B_W$ of f has the following block form:

$$M_{BB}(f) = \begin{pmatrix} M_{B_V B_V}(f) & 0 \\ 0 & M_{B_W B_W}(f) \end{pmatrix}.$$

7 Quotient Spaces

7.1 Definition of a Quotient Space

For a vector space V with $W \subseteq V$ a subspace. We define an equivalence relation on V by declaring:

$$v_1 \sim v_2 \text{ if } v_1 - v_2 \in W.$$

The set of equivalence classes is called the quotient of V by W and is denoted by V/W. For some v in V, we denote the class containing v by $v + W$ (similarly to cosets in Introduction to Group Theory). So, we have:

$$V/W = \{v + W : v \in V\},$$

with addition and multiplication defined for v_1, v_2 in V and a in the field:

$$(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W$$
$$a(v_1 + W) = av_1 + W.$$

7.2 Linear Map to the Quotient Space

For a vector space V with $W \subseteq V$ a subspace, we can define $\pi : V \to V/W$ for some v in V by $f(v) = v + W$. We have that π is linear and its kernel is W.

7.3 Isomorphisms formed by Linear Maps

For V, W vector spaces and $f : V \to W$ a linear map, we have an isomorphism $\mathrm{Im}(f) \cong V/\mathrm{Ker}(f)$.

7.4 Existence of a Linear Operator on the Quotient Space

For a vector space V with $W \subseteq V$ a subspace and a linear operator $f : V \to V$, there exists a well-defined operator $\bar{f} : V/W \to V/W$; $v + W \mapsto f(v) + W$ if and only if W if f-invariant. We call this the induced operator on V/W.

7.5 Matrices formed using Quotient Spaces

Consider a finite-dimension vector space V and $f : V \to V$ a linear operator with W an f-invariant subspace of V. If we have B_W a basis for W, that we extend to a basis B of V and set A:

$$A = \{v + W : v \in B \setminus B_W\},$$

a basis of V/W and we can form a matrix in block form:

$$M_{BB}(f) = \begin{pmatrix} M_{B_W B_W}(f) & * \\ 0 & M_{AA}(\bar{f}) \end{pmatrix},$$

where $\bar{f}$ is the induced operator on V/W and $*$ marks the area of the matrix which we cannot determine.

8 Dual Spaces

8.1 Definition of a Dual Space

For V a vector space over $\mathbb{F}$, we have that the dual space V^* is $\mathcal{L}(V, \mathbb{F})$, the set of linear maps from V to $\mathbb{F}$. We have that addition and scalar multiplication are defined for some v in V, f, g in V^*, and a in $\mathbb{F}$:

$$\begin{aligned}(f+g)(v) &:= f(v) + g(v), \\ (af)(v) &:= af(v).\end{aligned}$$

8.2 Definition of a Dual Basis

For V a finite-dimensional vector space over $\mathbb{F}$, with $\dim(v) = n$ and a basis $B = \{v_1, \ldots, v_n\}$. We define the dual basis $B^* = \{v_1^*, \ldots, v_n^*\}$ by defining $v_i^* : V \to \mathbb{F}$ as the unique linear map such that:

$$v_i^*(v_j) := \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j. \end{cases}$$

Equivalently, for v in V, we have that there's unique $(a_1, \ldots, a_n)$ in $\mathbb{F}$ such that:

$$v = \sum_{i=1}^{n} a_i v_i,$$

so we let v_i be such that:

$$v_i^*(v) = v_i^* \left(\sum_{j=1}^{n} a_j v_j \right) = \sum_{j=1}^{n} a_j v_i^*(v_j).$$

We have that B^* is a basis for V^*. Additionally, we have that V and V^* are isomorphic by the isomorphism mapping v_i to v_i^*.

8.3 Definition of the Annihilator

For V a vector space over $\mathbb{F}$ with $S \subseteq V$, the annihilator of S is the subspace S^0 of V^* where for f in S^0, $S \subseteq \mathrm{Ker}(f)$ (or rather, for all s in S, $f(s) = 0$).

8.4 Properties of the Annihilator

For V a vector space with $U, W \subseteq V$ subspaces, we have that:

- $(U + W)^0 = U^0 \cap W^0$
- $U \subseteq W \Rightarrow W^0 \subseteq U^0$,

and for V finite-dimensional,

- $(U \cap W)^0 = W^0 + U^0$
- $\dim(W) + \dim(W^0) = \dim(V)$.

8.5 Isomorphism to the Double Dual Space

For V a finite-dimensional vector space over $\mathbb{F}$, we have $F : V \to V^{**}$. That is:

$$V^{**} = \mathcal{L}(V^*, \mathbb{F}) = \mathcal{L}(\mathcal{L}(V, \mathbb{F}), \mathbb{F}),$$

so for some v in V we have:

$$F(v) : V^* \to \mathbb{F}.$$

We define F for some f in V^* as follows:

$$F(v)(f) = f(v).$$

We have that F is an isomorphism.

8.6 Definition of the Transpose

For V, W vector spaces with $f : V \to W$ a linear map. We define the transpose as $f^t : W^* \to V^*$ where for g in W^*, v in V:

$$f^t(g) := (g \circ f).$$

So, for some v in V:

$$f^t(g)(v) = (g \circ f)(v) = g(f(v)).$$

8.7 The Transpose and Matrices

If we have V, W finite-dimensional vector spaces over $\mathbb{F}$ with bases $A = \{v_1, \ldots, v_n\}$, $B = \{w_1, \ldots, w_m\}$ and corresponding dual bases $A^* = \{v_1^*, \ldots, v_n^*\}$, $B^* = \{w_1^*, \ldots, w_m^*\}$ respectively, we have that for some linear map $f : V \to W$, and $f^t : W^* \to V^*$ the transpose map:

$$M_{BA}(f) = \left(M_{A^*B^*}(f^t)\right)^t.$$

That is, for a given map, the matrix of transpose map is itself the matrix transpose of the matrix of the map.

9 Rank and Determinants

9.1 Elementary Row Operations

For a field $\mathbb{F}$, take A in $M_{m,n}(\mathbb{F})$. The elementary row operations are:

- Swapping
- Multiplying by scalars in $\mathbb{F} \setminus \{0_{\mathbb{F}}\}$
- Adding a multiple of a row to another

9.2 Elementary Matrices

The $n \times n$ elementary matrices are:

- $E_1(i, j)$: obtained by swapping the i^{th} and j^{th} rows of the identity
- $E_2(c, i)$: obtained by scaling the i^{th} row of the identity by c non-zero
- $E_3(c, i, j)$: obtained by adding c times row i to row j where $i \neq j$.

We have that any elementary row operation can be realised as left-multiplication by a corresponding elementary matrix. As a consequence of the definition, we have that elementary matrices are invertible and have elementary inverses.

9.3 Echelon Form

A matrix A is in echelon form if each row has the form:

$$(0, \dots, 0, 1, *, \dots, *),$$

where each row has more leading zeroes than the one above and the first row has any amount of leading zeroes. Every matrix can be put in this form via Gaussian elimination.

9.4 Decomposition via Elementary Matrices

For an $n \times n$ matrix A, there exists elementary matrices $E_1, \dots, E_k$ such that $E_1 \cdots E_k A = B$ where:

$$B = \begin{cases} \text{the identity} & \text{if } A \text{ is invertible} \\ \text{a matrix with a final row consisting of all zeroes} & \text{otherwise.} \end{cases}$$

9.5 Rank

For $A = (a_{ij})$ a matrix in $M_{m,n}(\mathbb{F})$, we denote its rows by $A_{(1)}, \dots, A_{(m)}$ and columns by $A^{(1)}, \dots, A^{(n)}$. We say:

- The row rank of A is the dimension of the subspace of spanned by $A^t_{(1)}, \dots, A^t_{(m)}$ in $\mathbb{F}^m$
- The column rank of A is the dimension of the subspace of spanned by $A^{(1)}, \dots, A^{(n)}$ in $\mathbb{F}^n$.

We have these are equal, so can generally refer to the rank of a matrix.

If $E_1, \dots, E_k$ are elementary matrices, we have that the rank of A is equal to the rank of $E_1 \cdots E_k A$. Similarly, similar matrices have the same rank.

9.6 Rank of Matrices from Linear Maps

For A an $m \times n$ matrix on $\mathbb{F}$, we can define a map $f : \mathbb{F}^n \to \mathbb{F}^m$ by $v \mapsto Av$. We have that the rank of A is the dimension of the image of f. Thus, invertible $n \times n$ matrices have rank n.

9.7 Permutations

9.7.1 Definition of a permutation

Let $[n]$ be $\{1, 2, \dots, n\}$. A permutation of $[n]$ is a bijection $\sigma : [n] \to [n]$. We define the set of all permutations on $[n]$ as S_n.

9.7.2 Decomposition of permutations

All permutations can be written as a product of disjoint cycles. Thus, all permutations can be written as a product of transpositions.

9.7.3 Definition of the parity of permutations

Even permutations are permutations that can be expressed as the product of an even number of transpositions. Otherwise, a permutation is odd.

9.7.4 The sgn function

We define the sgn function for a given permutation σ:

$$\mathrm{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{otherwise.} \end{cases}$$

We have that for another permutation τ:

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau).$$

In other words, sgn *is a homomorphism from* S_n *to* $\{1, -1\}$.

9.7.5 The alternating group

We have that A_n the set of even permutations in S_n is a subgroup as it is the kernel of sgn.

9.8 Determinants

9.8.1 Definition of a determinant

For $A = (a_{ij})$ a $n \times n$ matrix over $\mathbb{F}$, we have the determinant is a scalar defined by:

$$\det(A) := \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n}.$$

A more efficient but equivalent definition would be:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(\tilde{A}^{ij}),$$

where i is in $\{1, \ldots, n\}$ and $\tilde{A}^{ij}$ is A with the i^{th} row and j^{th} column removed.

We may represent the k^{th} column vector of A by $A^{(k)}$ and then write:

$$\det(A) = \det(A^{(1)}, \ldots, A^{(n)}).$$

9.8.2 Multi-linearity of the determinant

For $A = (a_{ij})$ a $n \times n$ matrix over $\mathbb{F}$ with $A_{(k)} = c_1 v_1 + c_2 v_2$ with c_1, c_2 in $\mathbb{F}$ and v_1, v_2 in $\mathbb{F}^n$, we have that:

$$\begin{aligned} \det(A) &= \det(A^{(1)}, \ldots, A^{(n)}) \\ &= c_1 \cdot \det(A^{(1)}, \ldots, v_1, \ldots, A^{(n)}) \\ &\quad + c_2 \cdot \det(A^{(1)}, \ldots, v_2, \ldots, A^{(n)}). \end{aligned}$$

From this we can show that any square matrix with a column of all zeroes has determinant zero.

9.8.3 Alternativity of the determinant

For $A = (a_{ij})$ a $n \times n$ matrix over $\mathbb{F}$ with $i \neq j$, we have that:

$$\begin{gathered} \det(A^{(1)}, \ldots, A^{(i)}, \ldots, A^{(j)} \ldots, A^{(n)}) \\ = \\ -\det(A^{(1)}, \ldots, A^{(j)}, \ldots, A^{(i)} \ldots, A^{(n)}). \end{gathered}$$

From this we can show that a matrix with a pair of identical columns must have zero determinant.

9.8.4 Normality of the determinant

For a square upper (or lower) triangular matrix A, we have that the determinant is the product of the diagonal entries.

From this we can show that the determinant of the identity is 1.

9.8.5 The determinants of elementary matrices

We have the following:

$$\begin{aligned} \det\left[E_1(i,j)\right] &= -1 \\ \det\left[E_2(c,i)\right] &= c \\ \det\left[E_3(c,i,j)\right] &= 1. \end{aligned}$$

9.8.6 The determinant of the transpose

For a matrix A, we have that: $\det(A) = \det(A^t)$.

9.8.7 The determinant under matrix multiplication

For A, B two $n \times n$ matrices, we have that: $\det(AB) = \det(A) \cdot \det(B)$.

9.8.8 The determinant and invertibility

A square matrix is invertible if and only if it has non-zero determinant.

10 Polynomials

10.1 Definition of a Polynomial

For R a ring, a polynomial over R is of the form:

$$p(x) = \sum_{i=0}^{n} a_i x^i,$$

for some sequence (a_i) in R called the coefficients of the polynomial. In this case, x is the interdeterminate.

$R[x]$ is the set of all polynomials on R.

10.2 Definition of the Degree of a Polynomial

For a polynomial p with coefficients (a_i) the degree is the greatest i such that $a_i \neq 0$ and if no such a_i exists we call this the zero polynomial. The degree is denoted as $\deg(p)$.

The leading coefficient is $a_{deg(p)}$.

10.3 Degree and Composition in $R[x]$

For p, q non-zero elements of $R[x]$, we have that:

- $\deg(p + q) \leq \max(\deg(p), \deg(q))$
- $\deg(pq) \leq \deg(p) + \deg(q)$
- $\deg(pq) = \deg(p) + \deg(q)$ if the leading coefficient of p or q is an invertible element of R (or R is a field).

10.4 Multiplication in $R[x]$

We have that $R[x]$ is commutative if and only if R is commutative. Also, we have that $R[x]$ has a multiplicative identity if and only if R has one.

10.5 Evalutation of Polynomials

For $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ in $R[x]$ and c in R, we have the value of p at c is:

$$p(c) = a_0 + a_1 c + \cdots + a_n c^n.$$

If $p(c) = 0$, then we call c a root of p.

10.6 The Division Algorithm of Polynomials

For f, g in $R[x]$ with the leading coefficient of g being a unit (invertible element) in R, we have that there exists q, r in $R[x]$ such that:

$$f(x) = q(x)g(x) + r(x),$$

where r is the zero polynomial or $\deg(r) < \deg(g)$.

10.7 Factorisation by Roots

For p a polynomial in $R[x]$ where $\deg(p) > 0$ and c in R:

$$p(c) = 0$$
$$\iff$$
$$\exists\, q \in R[x] \text{ such that } p(x) = q(x) \cdot (x - c).$$

10.8 Division of Polynomials

For a field K, we have that for p, q in $K[x]$, if q divides p (written as $q|p$) then there exists r in $K[x]$ such that:

$$p(x) = q(x)r(x).$$

10.9 Highest Common Factors of Polynomials

For a field K, we have that for p, q in $K[x]$, the highest common factor of p and q is a polynomial h with **maximal** degree such that h divides both p and q.

We also have that there exists a, b in $K[x]$ such that $h = ap + bq$.

10.10 Irreducible Polynomials

An irreducible polynomial over a field K is a non-constant polynomial in $K[x]$ such that it cannot be written as the product of two polynomials (both with smaller degree).

10.11 Decomposition into Irreducible Polynomials

For a field K, we have that for every f in $K[x]$, where $\deg(f) \geq 1$ we have that f can be written as the product of irreducible polynomials unique up to order and multiplication by constants. If f is monic (leading coefficient equal to one), it is a product of monic irreducible polynomials, unique up to order.

10.12 Definition of the Minimal Polynomial

For a field K, V a finite dimensional vector space with $\dim(V) = n$, let f be in $\mathrm{End}(V) = \mathcal{H}(V, V)$ (homomorphisms from V to V). The minimal polynomial $m_f(x)$ in $K[x]$ is the polynomial such that:

- $m_f(f) = 0$ in $\mathrm{End}(V)$
- $\deg(m_f)$ is minimal
- m_f is monic (leading coefficient equal to one).

We have that this polynomial always exists and is unique.

For each p in $K[x]$, it's important to see that $p(f)$ is in End(V).

10.13 Properties of the Minimal Polynomial

For a field K, V a finite dimensional vector space with $\dim(V) = n$, let f be in $\mathrm{End}(V)$ and m_f be the corresponding minimal polynomial in $K[x]$. We have that:

- If p in $K[x]$ satisfies $p(f) = 0$ then $m_f | p$
- For λ in K, $m_f(\lambda) = 0$ if and only if λ is an eigenvalue of f

10.14 Definition of the Characteristic Polynomial

The characteristic polynomial of an operator $f : V \to V$ is the polynomial:

$$p_f(x) = \det(A - xI),$$

where A is the matrix of f relative to some basis.

This doesn't change based on the choice of basis and similar matrices have the same determinant.

Also, this is divisible by m_f by the Cayley-Hamilton theorem.

10.15 The Cayley-Hamilton Theorem

For V a finite dimensional vector space over a field $\mathbb{F}$ where p_f the characteristic polynomial of an operator $f : V \to V$, we have that:

$$p_f(f) = 0_V.$$

We also have that:

$$p_f(M_{BB}(f)) = 0_V,$$

for some basis B of V.

10.16 Definition of a Root Vector

For a finite dimensional vector space V over $\mathbb{F}$, with $f : V \to V$, and λ in $\mathbb{F}$, we have that v in V is a λ-root vector of v if there exists n in $\mathbb{N}$ such that:

$$(f - \lambda(\mathrm{id}))^n v = 0.$$

The smallest such n is the height of v denoted by $h(v)$.

The set $V(\lambda)$ of all root vectors corresponding to λ is the root space of λ.

10.16.1 Properties of the Root Space

We have the following properties:

- $V(\lambda)$ is a subspace
- $V(\lambda) \neq \{0\}$ if and only if λ is an eigenvalue of f
- $V(\lambda)$ is f-invariant.

10.17 Primary Decomposition Theorem

For a finite dimensional vector space V over $\mathbb{F}$ (algebraically closed) we have that:

$$V = \bigoplus_{i \in [n]} V(\lambda_i),$$

where $\{\lambda_1, \dots, \lambda_n\}$ is the set of eigenvalues of a linear operator.

10.18 Definition of a Jordan Block

For a field $\mathbb{F}$, h in $\mathbb{N}$, a Jordan block of size $h \times h$ on λ in $\mathbb{F}$ is the matrix of the form:

$$J_h(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \lambda & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix},$$

or alternatively:

$$J_h(\lambda) = (a_{ij}),\ a_{ij} = \begin{cases} \lambda & i = j \\ 1 & j = i + 1 \\ 0 & \text{otherwise.} \end{cases}$$

10.19 Definition of a Jordan Matrix

For a field $\mathbb{F}$, a Jordan matrix consisting of Jordan blocks of sizes $\{h_1, \dots, h_n\}$ in $\mathbb{N}$ and values $\{\lambda_1, \dots, \lambda_n\}$ in $\mathbb{F}$ has the form:

$$J = \begin{pmatrix} J_{h_1}(\lambda_1) & 0 & \cdots & 0 \\ 0 & J_{h_2}(\lambda_2) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & J_{h_n}(\lambda_n) \end{pmatrix}$$

10.19.1 Definition of Jordan Normal Form

A Jordan normal form of a matrix A is a Jordan matrix that is similar to A.

10.20 Definition of a Jordan Basis

For an algebraically closed field $\mathbb{F}$, a finite dimensional vector space V over $\mathbb{F}$, with f in $\mathrm{End}(V)$, we have that a basis B of V is a Jordan basis for f if:

$$M_{BB}(f) \text{ is Jordan.}$$

10.21 Definition of Nilpotence

For a field $\mathbb{F}$, a finite dimensional vector space V over $\mathbb{F}$, with f in $\mathrm{End}(V)$, we have that f is nilpotent if there exists r in $\mathbb{Z}_{>0}$ such that $f^r = 0$ in $\mathrm{End}(V)$.

We have that 0 is the only eigenvalue of nilpotent maps, thus for some m, m' in $\mathbb{Z}_{>0}$ with $m' \leq m$:

- $p_f(x) = x^m$
- $m_f(x) = x^{m'}$
- $V = V(0)$, the zero eigenspace.

10.22 Nilpotent Maps on Eigenspaces

Let $\mathbb{F}$ be a field, V be a finite dimensional vector space over $\mathbb{F}$, f be in $\mathrm{End}(V)$, λ be an eigenvalue of f. Let $g : V(\lambda) \to V(\lambda)$ be $g(v) = f(v)$ for v in $V(\lambda)$. So, we have that $(g - \lambda \mathrm{id})$ is nilpotent.

10.23 Existence of Jordan Bases

Let $\mathbb{F}$ be an algebraically closed field, V be a finite dimensional vector space over $\mathbb{F}$, f be in $\mathrm{End}(V)$, thus there exists a Jordan basis for f.

10.24 Uniqueness of Jordan Matrices

For an algebraically closed field $\mathbb{F}$, a finite dimensional vector space V over $\mathbb{F}$, with f in $\mathcal{L}(V, V)$, we have that the Jordan form of the matrix of f is uniquely determined up to the permutations of the Jordan blocks.

11 Bilinear and Quadratic Forms

11.1 Definition of a Bilinear Form

For V a vector space over a field K, a bilinear form on V is a map $\langle\, , \rangle : V \times V \to K$ such that:

$$\begin{aligned}\langle au + bv, w\rangle &= a \cdot \langle u, w\rangle + b \cdot \langle v, w\rangle \\ \langle u, av + bw\rangle &= a \cdot \langle u, v\rangle + b \cdot \langle u, w\rangle,\end{aligned}$$

for all a, b in K, u, v, w in V. Additionally, $\langle\, , \rangle$ is symmetric if $\langle u, v\rangle = \langle v, u\rangle$.

11.2 Definition of a Quadratic Form

For V a vector space over a field K with $\langle\, , \rangle$ a symmetric bilinear form on V. The quadratic form $Q : V \to K$ associated to $\langle\, , \rangle$ is $Q(v) := \langle v, v\rangle$.

11.2.1 Determining bilinear forms from quadratic forms

We have that if $\mathrm{char}(K) \neq 2$, then $\langle\, , \rangle$ is uniquely defined by Q as:

$$\langle v, w\rangle = 2^{-1} \left[Q(v + w) - Q(v) - Q(w)\right].$$

11.3 Definition of Orthogonality

Let $\langle\, , \rangle$ be a bilinear form on V with v in V. We say that u in V is orthogonal to v if $\langle v, u\rangle = 0$. Note, be very careful as the bilinear is not necessarily symmetric.

11.3.1 Definition of orthogonal spaces

For $W \subseteq V$, we have that $W^{\perp}$ is defined as:

$$W^{\perp} = \{v \in V : w \in W, \langle w, v\rangle = 0\},$$

the set of vectors such that for all v in $W^{\perp}$, v is orthogonal to all of W. This is a subspace of V.

11.3.2 Definition of the kernel for bilinear maps

The kernel of $\langle\, , \rangle$ is $V^{\perp}$. If the kernel is $\{0_V\}$, then the form is called non-degenerate and is called degenerate otherwise.

11.3.3 Dimension and orthogonal spaces

We have that if V is finite dimensional and $\langle\,,\rangle$ is non-degenerate then:

$$\dim(W^{\perp}) + \dim(W) = \dim(V).$$

11.4 Linear Maps from Bilinear Forms

We can form a linear map $f : V \to V^*$ from a bilinear form $\langle\,,\rangle$ as follows:

$$f(v)(u) = \langle u, v\rangle.$$

We have that a bilinear form is non-degenerate if and only if its corresponding linear map is an isomorphism.

11.4.1 Isomorphismic Bilinear Maps

If V is finite dimensional, we have that f is an isomorphism if and only if $\langle\,,\rangle$ is non-degenerate. That is, $\mathrm{Ker}(f) = \mathrm{Ker}(\langle\,,\rangle) = V^{\perp}$.

11.5 Matrices from Bilinear Forms

For V a finite n-dimensional vector space over K with $S = \{v_1, \ldots, v_n\}$ an ordered basis for V. Let $B = \langle\,,\rangle$ be a bilinear form. The matrix corresponding to B with respect to S is $M_{SS}(B) = (b_{ij})$ where:

$$b_{ij} = \langle v_i, v_j\rangle.$$

Similarly, taking $S^* = \{v_1^*, \ldots, v_n^*\}$ to be a dual basis for S^*, we have a matrix $M_{SS^*}(f) = M_{SS}(B)$ for the linear map corresponding to B.

11.5.1 Determining bilinear forms from matrices

Take u, v in V decomposed into vectors in S with coefficients $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ respectively. Thus:

$$\langle u, v\rangle = (x_1, \ldots, x_n) \cdot M_{SS}(B) \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

11.5.2 Properties of matrices of bilinear forms

We have that:

- If $M_{SS}(B)$ is symmetric, so is B
- B is non-degenerate if and only if $M_{SS}(B)$ is invertible.

11.6 Similarity of Matrices of Bilinear Forms

For V a finite n-dimensional vector space over the field K with $\mathrm{char}(K) \neq 2$, let $S = \{v_1, \ldots, v_n\}$, $S' = \{v'_1, \ldots, v'_n\}$ be ordered bases for V. Let $B = \langle\, , \rangle$ be a symmetric bilinear form. Let $C = C_{SS'}$ be the transition matrix. We have that:

$$M_{S'S'}(B) = C^t M_{SS}(B) C.$$

11.7 Diagonal Matrices of Bilinear Forms

For V a finite n-dimensional vector space over the field K with $\mathrm{char}(K) \neq 2$, let $B = \langle\, , \rangle$ be a symmetric bilinear form. There exists a basis $S = \{v_1, \ldots, v_n\}$ for V consisting of pairwise orthogonal vectors and thus, the matrix $M_{SS}(B)$ is diagonal.

11.8 Definition of an Inner Product

For a vector space V over K with symmetric bilinear form $B : V \times V \to K$, we have that B is an inner product if for all v in V:

$$B(v, v) \geq 0,$$

and $B(v, v) = 0$ if and only if $v = 0_V$.