MAT 442: Advanced Linear Algebra

Arizona State University

Fall 2020

Contents

1 Vector Spaces

1.1 Fields

Definition 1 A *field* is a triple $(\mathbb{F}, +, \cdot)$ with $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ and $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ that satisfies the following axioms.

(1) For all $a, b, c \in \mathbb{F}$, $(a + b) + c = a + (b + c)$ (Associativity of addition)

(2) For all $a, b, c \in \mathbb{F}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Associativity of multiplication)

(3) For all $a, b \in \mathbb{F}$, $a + b = b + a$ (Commutativity of addition)

(4) For all $a, b \in \mathbb{F}$, $a \cdot b = b \cdot a$ (Commutativity of multiplication)

(5) For all $a, b, c \in \mathbb{F}$, $a \cdot (b + c) = a \cdot b + a \cdot c$ (Distributive law)

(6) There exists $0 \in \mathbb{F}$ such that $a + 0 = a$ for all $a \in \mathbb{F}$ (Identity element of addition)

(7) There exists $0 \in \mathbb{F}$ such that $a \cdot 0 = a$ for all $a \in \mathbb{F}$ (Identity element of multiplication)

(8) For all $a \in \mathbb{F}$, there exists $(-a) \in \mathbb{F}$ such that $a + (-a) = 0$ (Additive inverse)

(9) For all $a \in \mathbb{F}$, there exists $a^{-1} \in \mathbb{F}$ such that $a \cdot a^{-1} = 0$ (Multiplicative inverse)

Examples of Fields

(1) $(\mathbb{R}, +, \cdot)$

(2) $(\mathbb{C}, +, \cdot)$

(3) $(\mathbb{Q}, +, \cdot)$

(4) $(\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}, +, \cdot)$

(5) $(\mathbb{Z}_2, +, \cdot)$

(6) $(\mathbb{Z}_p, +, \cdot)$, where p prime

1.2 Vector Spaces

Definition 1 A *vector space* V over a field F is a triple $(V, +, \cdot)$ where $+ : V \times V \to V$ (addition), $\cdot : F \times V \to V$ (scalar multiplication) and the following conditions hold.

(VS 1) For $x, y \in V$, $x + y = y + x$ (Commutativity of addition)

(VS 2) For $x, y, z \in V$, $(x + y) + z = x + (y + z)$ (Associativity of addition)

(VS 3) There exists an element $0_V \in V$ such that $0_V + x = x$ for all $x \in V$ (Identity element of addition)

(VS 4) For $x \in V$, there is $y_x \in V$ such that $x + y_x = 0_V$ (Inverse elements of addition)

(VS 5) For $x \in V$, $1 \cdot x = x$ (Identity element of scalar multiplication)

(VS 6) For $a, b \in \mathbb{F}$, $x \in V$, $(ab)x = a(bx)$ (Compatibility of scalar multiplication)

(VS 7) For $a \in \mathbb{F}$, $x, y \in V$, $a(x + y) = ax + ay$ (Distributivity of scalar multiplication with respect to vector addition)

(VS 8) For $a, b \in \mathbb{F}$, $x \in V$, $(a + b)x = ax + bx$ (Distributivity of scalar multiplication with respect to field addition)

Conventions

- We will often identify the set V with the vector space V.
- We will write av instead of $a \times v$.
- We will often write 0 for 0_V when V is clear from the context.

An $m \times n$ matrix with entries from a field F is a function $A : \{1, \ldots, m\} \times \{1, \ldots, n\} \to \mathbb{F}$. We often organize the values in a rectangular array with m rows and n columns and use A_{ij} for $A(i, j)$.

Examples of Vector Fields

(1) $\mathbb{F}^n = \{(a_1, \ldots, a_n) : a_i \in \mathbb{F}\}$

(2) $\{f : S \to \mathbb{F} : S \neq \emptyset\}$. Also notated $\mathcal{F}(S, F)$.

(3) Set of all sequences over $\mathbb{F}$

(4) $P(\mathbb{F})$. Set of all polynomials with coefficients in $\mathbb{F}$.

(5) $M_{m \times n}(\mathbb{F})$

Example: Is the empty set a vector space?

Answer. No. By rule (VS 3), there must exist $0_V \in V$, such that $0_V + x = x$ for all $x \in V$, but since $V = \emptyset$, $\nexists 0_V \in V$.

Example: Decide if V is a vector space.

(1) $V = \{(a_1, a_2) : a_1, a_2 \in \mathbb{R}\}$, $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 - b_2)$, $c(a_1, a_2) = (ca_1, ca_2)$

Answer. No. V violates axiom (VS 1).

(2) $V = \{(a_1, a_2) : a_1, a_2 \in \mathbb{R}\}$, $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, 0)$, $c(a_1, a_2) = (ca_1, 0)$

Answer. No. V violates axiom (VS 5).

(3) $V = \{(a_1, a_2) : a_1, a_2 \in \mathbb{R}\}$, $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 b_2)$, $c(a_1, a_2) = (ca_1, a_2)$

Answer. No. V violates axiom (VS 4).

Theorem 1.1. (Cancellation Law for Vector Addition) Let $x, y, z \in V$. If $x + z = y + z$, then $x = y$.

Proof. Suppose $x + z = y + z$. Let w be such that $z + w = 0_V$. Then

$$\begin{aligned} x &= x + 0_V \\ &= x + (z + w) \\ &= (x + z) + w \\ &= (y + z) + w \\ &= y + (z + w) \\ &= y + 0_V \\ &= y. \end{aligned}$$

□

Corollary 2

- There is unique $0_V \in V$ such that $0_V + x = x$ for all $x \in V$.

  Proof. Let $v \in V$. Suppose that 0_V and $0'_V$ are zero elements.

  $$v + 0_V = v = v + 0'_V.$$

  Thus, by cancellation law, $0_V = 0'_V$. □

- For every $x \in V$, there is unique $y_x \in V$ such that $x + y_x = 0_V$. *Proof.* Let $x \in V$. Suppose that y_x and y'_x are inverses of x. Then

$$x + y_x = 0 = x + y'_x.$$

Thus, by cancellation law, $y_x = y'_x$. □

Theorem 1.2. Let $x \in V$, $a \in \mathbb{F}$. Then

- $0x = 0_V$;

  Proof.

$$\begin{aligned} 0x + 0x &= (0+0)x \\ &= 0x \\ &= 0x + 0_V. \end{aligned}$$

Thus, by cancellation law, $0x = 0_V$. □

- $(-a)x = -(ax) = a(-x)$;

  Proof. We can show

$$\begin{aligned} (-a)x + (ax) &= (-a+a)x \\ &= 0x \\ &= 0_V. \end{aligned}$$

Thus, the inverse of ax is unique, which implies $-ax = (-a)x$. We have $(-x) = (-1)x$, which implies $a(-x) = (a(-1))x = (-a)x$. □

- $a0_V = 0_V$.

  Proof.

$$a0_V = a(0_V - 0_V) = a0_V - a0_V = 0_V.$$

□

1.3 Subspaces

Definition 2 Let $(V, +, \cdot)$ be a vector space and let $W \subseteq V$. Then W is called a *subspace* if $(W, +, \cdot)$ is a vector space.

Note: W is a subspace if

- $x + y \in W$ for $x, y \in W$

- $cx \in W$ for $x \in W$, $c \in \mathbb{F}$
- W has a zero vector 0_W
- For $x \in W$ there is $y_x \in W$ such that $x + y_x = 0_W$

Theorem 1.3. Let W be a subset of V a vector space $(V, +, \cdot)$. Then W is a subspace of V if and only if the following hold.

(1) $0_V \in W$

(2) if $x, y \in W$, then $x + y \in W$

(3) if $c \in \mathbb{F}$ and $x \in W$, then $cx \in W$

Proof. ($\Longrightarrow$): Suppose W is a subspace. Then (2) and (3) are satisfied. Then, $0_W + 0_W = 0_W = 0_W + 0_V$. Thus, by cancellation law, $0_W = 0_V$.

($\Longleftarrow$): Suppose $x \in W$. We have $-x = (-1)x$ and $-1 \in \mathbb{F}, x \in W$. Thus, $-x \in W$. $\square$

The *transpose* of an $m \times n$ matrix A is the $n \times m$ matrix A^t such that $(A^t)_{ij} = A_{ji}$. Note, $(A + B)^t = A^t + B^t$. Also, $(cA^t) = cA^t$. This is proven by,

$$\begin{aligned} ((A+B)^t)_{ij} &= (A+B)_{ji} \\ &= A_{ji} + B_{ji} \\ &= (A^t)_{ij} + (B^t)_{ij}. \end{aligned}$$

A is called *symmetric* if $A^t = A$.

An $n \times n$ matrix A is called *diagonal* if $A_{ji} = 0$ whenever $j \neq i$.

Theorem 1.4. Any intersection of subspaces of a vector space V is a subspace of V.

Definition 3

- Let $S_1, S_2 \subseteq V$. Then $S_1 + S_2$ is the set $\{x + y : x \in S_1, y \in S_2\}$
- V is called a direct sum of W_1 and W_2 if W_1, W_2 are subspaces of V such that $W_1 \cap W_2 = \{0\}$ and $W_1 + W_2 = V$. We then write $V = W_1 \oplus W_2$.

  Example: Let $V = \mathbb{R}^2$, $S_1 = \{(a, 0) : a \in \mathbb{R}\}$, $S_2 = \{(0, b) : b \in \mathbb{R}\}$. Then $S_1 + S_2$ generates V.

Examples of subspaces

(1) $\mathcal{C} = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : f \text{ is continuous}\}$ is a subspace of $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

(2) $P_n(\mathbb{R}) = \{f : f \text{ is a polynomial and } deg(f) \leq n\}$ is a subspace of $P(\mathbb{R})$.

(3) $D = \{A \in M_{n\times n}(\mathbb{R}) : A \text{ is diagonal}\}$ is a subspace of $M_{n\times n}(\mathbb{R})$.

(4) $W = \{A \in M_{n\times n}(\mathbb{R}) : tr(A) = 0\}$ is a subspace of $M_{n\times n}(\mathbb{R})$.

1.4 Linear combinations and systems of linear equations

Definition 4 Let S be a subset of a vector space V and let $v \in V$. Then v is called a linear combination of vectors of S if there exists $u_1, \dots, u_n \in S$ and $a_1, \dots, a_n \in \mathbb{F}$ such that

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

When solving a system of linear equations we reduced to what is called the reduction echelon form by performing the following three operations.

- Interchange two equations
- Multiply an equation by a non-zero element from F
- Add a scalar multiple of one equation to another

Example: $v = (2, 6, 8) \in \mathbb{R}^3$ is a linear combination of $v_1 = (1, 2, 1)$, $v_2 = (-2, -4, -2)$, $v_3 = (0, 2, 3)$, $v_4 = (2, 0, -3)$, $v_5 = (-3, 8, 16)$. Specifically, $v = a_1 v_1 + \cdots + a_5 v_5$ where $(a_1, a_2, a_3, a_4, a_5) = (-4, 0, 7, 3, 0)$ is one solution.

Definition 5 Let S be a subset of a vector space V. If S is non-empty, we let $span(S)$ be the set of all linear combinations of vectors from S, and we set $span(\emptyset) = \{0_V\}$.

Theorem 1.5. Let S be a subset of a vector space V. Then $span(S)$ is a subspace of V. Moreover, if W is a subspace of V such that $S \subseteq W$, then $span(S) \subseteq W$.

Proof.

(1) (Show $span(S)$ is a subspace): If $S = \emptyset$, then $span(S) = \{0_V\}$, which is a subspace. Assume $S \neq \emptyset$. Let $v \in S$. Then,

(a) $0v = 0_V \in span(S)$

(b) Suppose $x, y \in span(S)$. Then $x = \sum_{i=1}^{n} a_i v_i$, $y = \sum_{i=1}^{m} b_i w_i$ where $v_1, \dots v_n, w_1, \dots, w_m \in S$ and $a_1, \dots, b_1, \dots, b_m \in \mathbb{F}$. Let

$$u_i = \begin{cases} v_i & i \leq n \\ w_{i-n} & i > n \end{cases}, \qquad c_i = \begin{cases} a_i & i \leq n \\ b_{i-n} & i > n. \end{cases}$$

Then $x + y = \sum_{i=1}^{n+m} c_i u_i$ and $u_i \in S$, $c_i \in \mathbb{F}$ for $i = 1, \dots, n+m$. Thus, $x + y \in span(S)$.

(c) Let $x \in span(S)$ and let $c \in \mathbb{F}$. Then $x = \sum_{i=1}^{n} a_i v_i$ where $v_1, \dots, v_n \in S$ and $a_1, \dots, a_n \in \mathbb{F}$. Then $cx = \sum_{i=1}^{n} (ca_i) v_i$ and $ca_i \in \mathbb{F}$.

Therefore $span(S)$ is a subspace.

(2) Let $x \in span(S)$. Then, $x = \sum_{i=1}^{n} a_i v_i$, where $a_i \in \mathbb{F}$ and $v_i \in S$. We will use induction on n.

- If $n = 1$, $x = a_1 v_1$, and $v_1 \in W$. Thus, $x \in W$.
- Suppose $x = \sum_{i=1}^{n} a_i v_i$. Then $x = \sum_{i=1}^{n-1}(a_i v_i) + a_n v_n$. Then $\sum_{i=1}^{n-1}(a_i v_i) \in W$ by inductive hypothesis and $a_n v_n \in W$. Thus $x \in W$.

Therefore, $span(S) \subseteq W$.

$\square$

Note: In particular, $span(span(S)) = span(S)$.

Proof.

(a) $span(S) \subseteq span(span(S))$

(b) Let $x = span(S)$. Then $span(S) \subseteq span(S)$ implies $span(S) \subseteq x$, which gives us $span(span(S)) \subseteq span(S)$. Therefore, $(span(span(S)) = span(S)$.

$\square$

Definition 6 A subset S of V *generates* (spans) V if $span(S) = V$.

Example: Let $V = M_{2\times 2}(\mathbb{R})$ and $S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}$. Then $span(S) = V$.

1.5 Linear dependence and linear independence

Definition 7 A subset S of a vector space V is called *linearly dependent* if there exists distinct vectors $u_1, \ldots, u_n \in S$ and $a_1, \ldots, a_n \in \mathbb{F}$ not all zero such that $a_1 u_1 + \cdots + a_n u_n = 0$.

Notes:

- The empty set is linearly dependent.
- $S = \{u\}$ is linearly dependent if and only if $u \neq 0$.
- A set is called linearly independent if and only if the only representation of 0 as linear combinations of its vectors are trivial.

Theorem 1.6. Let $S_1 \subseteq S_2 \subseteq V$. If S_1 is linearly dependent, then so is S_2.

Example: Let $S = \{(1,0,0,-1),(0,1,0,-1),(0,0,1,-1),(0,0,0,1)\} \subseteq \mathbb{R}^4$. We'll show S is linearly independent. Suppose

$$a_1(1,0,0,-1) + a_2(0,1,0,-1) + a_3(0,0,1,-1) + a_4(0,0,0,1) = (0,0,0,0).$$

We get $a_1 = 0, a_2 = 0, a_3 = 0, -a_1 - a_2 - a_3 + a_4 = 0$, which implies $a_1 = a_2 = a_3 = a_4 = 0$.

Example: $P_k(x) = x^k + \cdots + x^n$ where $1 \leq k \leq n$. We'll show that $\{P_0(x), \ldots, P_n(x)\}$ is linearly independent. Suppose $a_0P_0(x) + \cdots + a_nP_n(x) = 0$. The coefficient of x^i on the left hand side is $a_0 + \cdots + a_i$. Then we have

$$\begin{aligned} a_0 + \cdots + a_n &= 0 \\ a_0 + \cdots + a_{n-1} &= 0 \\ &\vdots \\ a_0 &= 0. \end{aligned}$$

Thus, $a_0 = \cdots = a_n = 0$.

Corollary 8 If $S_1 \subseteq S_2 \subseteq V$ and S_2 is linearly independent, then so is S_1.

Theorem 1.7. Let S be a linearly independent subset of V and let $v \in V \setminus S$. Then $S \cup \{v\}$ is linearly dependent if and only if $v \in span(S)$.

Proof. Let S be linearly independent, $v \notin S$. We'll show $S \cup \{v\}$ is linearly dependent if and only if $v \in span(S)$.

($\Longrightarrow$): Suppose $T = S \cup \{v\}$ is linearly dependent. Then, there exists $a_1, \ldots, a_n$ not all zero and there exists $u_1, \ldots, u_n \in T$ such that $a_1u_1 + \cdots + a_nu_n = 0_V$. Since S is linearly independent, $u_i = v$ for some $1 \leq i \leq n$. Say $u_1 = v$ and $a_i \neq 0$. Then $a_1u_1 = -a_2u_2 - \cdots - a_nu_n$. Thus $u_1 = -\frac{a_2}{a_1}u_2 - \cdots - \frac{a_n}{a_1}u_n$. Also $u_2, \ldots, u_n \in S$. Therefore $u_1 \in span(S)$.

($\Longleftarrow$): Let $v \in span(S)$. Then there exists $a_1, \ldots, a_n$ not all zero and there exists $v_1, \ldots, v_n \in S$ such that $v = a_1v_1 + \cdots + a_nv_n$. Then $v - a_1v_1 - \cdots - a_nv_n = 0_V$. The coefficient on v is $1 \neq 0$. Thus, $\{v\} \cup S$ is linearly dependent. $\square$

1.6 Bases and dimension

Definition 8 A *basis* β for a vector space V is a linearly independent subset of V that generates V.

Theorem 1.8. Let V be a vector space and let $\beta = \{u_1, \ldots, u_n\}$. Then β is a basis of V if and only if each v can be uniquely written as

$$v = a_1u_1 + \cdots + a_nu_n$$

where $a_1, \ldots, a_n \in \mathbb{F}$.

Proof. ($\Longrightarrow$): Suppose $\beta = \{u_1, \ldots, u_n\}$ is a basis for a vector space V. Then $span(\beta) = V$ and every $v \in V$ can be written as a linear combination of $u_1, \ldots, u_n$. Suppose $v = \sum_{i=1}^n a_i u_i$ and $v = \sum_{i=1}^n b_i u_i$. Then $0_V = \sum_{i=1}^n (a_i - b_i)u_i$. Thus $a_i = b_i = 0$ for every $i = 1, \ldots, n$.

($\Longleftarrow$): Suppose every $v \in V$ can be written uniquely as $v = \sum_{i=1}^n a_i u_i$. Then $span(\{u_1, \ldots, u_n\}) = V$. Suppose $a_1u_1 + \cdots + a_nu_n = 0_V$. Note, $0_V = u_1 \cdot 0 + \cdots + u_n \cdot 0$. Since every vector has a unique representation as a linear vector, then $a_1 = \cdots = a_n = 0$. Thus, $\{u_1, \ldots, u_n\}$ is linearly independent and a basis for V. □

Theorem 1.9. Let S be a finite set that generates V. Then there is a subset of S which is a basis for V.

Proof. If $S = \emptyset$ or $S = \{0_V\}$, then $V = \{0_V\}$ and $\emptyset$ is a basis. Assume S contains a finite set of at least one nonzero vector v, which generates V. Then $\{v\}$ is linearly independent. Let $\{u_1, \ldots, u_k\}$ is a maximal linearly independent subset of S. Then $S \subseteq span(\{u_1, \ldots, u_k\})$. Then $span(S) \subseteq span(span(\{u_1, \ldots, u_k\}))$. So, $span(S) = V \subseteq span(\{u_1, \ldots, u_k\})$. Therefore $\{u_1, \ldots, u_k\}$ is a basis for V. □

Theorem 1.10. Let $G \subset V$, $|G| = n$ and $V = span(G)$. Suppose further that $L \subseteq V$, $|L| = m$ and L is linearly independent. Then $m \leq n$ and there exists a subset H of G such that $|H| = n - m$ and $L \cup H$ generates V.

Proof. (Outline)

- Induction on m. For the inductive step consider $L = \{v_1, \ldots, v_{m+1}\}$
- Apply induction to $\{v_1, \ldots, v_m\}$. Thus $m \leq n$ and there is a subset $H' \ldots$
- H' can't be empty, say $H' = \{u_1, \ldots, u_{n-m}\}$. Thus $m \leq n$.
- To find H for L, use the fact $H' \cup \{v_1, \ldots, v_m\}$ generates V and substitute one of vectors from H' with v_{m+1}.

Proof. Let $|G| = n$, $span(G) = V$, $|L| = m$, L is linearly independent. Then, using induction on m,

(Base Case): If $m = 0$, then $L = \emptyset$, $|L| = 0$ and $H = G$ and $|H| = n = n - 0$.

(Inductive Step): Suppose $L = \{v_1, \ldots, v_{m+1}\}$ is linearly independent. Let $L' = \{v_1, \ldots, v_m\}$. By inductive hypothesis, there exists $m \leq n$ and there exists $H' \subseteq G$, such that $|H'| = n-m$ and $span(L' \cup H') = V$. Note, $H' \neq \emptyset$. Otherwise, $span(L') = V$. In particular, $v_{m+1} \in span(\{v_1, \ldots, v_m\})$, but L is linearly independent, contradiction. Therefore, $H' \neq \emptyset$ and so $n - m > 0$. Thus, $m + 1 \leq n$. Say $H' = \{u_1, \ldots, u_{n-m}\}$. Since $span(L' \cup H') = V$,

$$v_{m+1} = \sum_{i=1}^{m} a_i v_i + \sum_{i=1}^{n-m} b_i u_i.$$

Now, at least one of scalars b_i is nonzero, say $b_1 \neq 0$. Then, $b_1 u_1 = v_{m+1} - \sum_{i=1}^{m} a_i v_i - \sum_{i=2}^{n-m} b_i u_i$. So,

$$u_1 = \frac{1}{b_1} v_{m+1} - \sum_{i=1}^{m} \frac{a_i}{b_1} v_i - \sum_{i=2}^{n-m} \frac{b_i}{b_1} u_i,$$

which implies $u_1 \in span(\{v_1, \dots, v_{m+1}\} \cup \{u_2, \dots, u_{n-m}\})$. Thus, $u_1 \in span(L \cup \{u_2, \dots, u_{n-m}\})$. Let $H = \{u_2, \dots, u_{n-m}\}$. Then $|H| = n - m - 1 = n - (m+1)$ and $H \subseteq G$. We have $u_i \in span(L \cup H)$ for $i = 1, \dots, n-m$ and $L \subseteq span(L \cup H)$. Thus, $V \subseteq span(L \cup \{u_1, \dots, u_{n-m}\}) \subseteq span(L \cup H)$. □

Corollary 13 Suppose V has finite basis. Then every basis for V has the same cardinality.

Proof. Let β and γ be bases for V.

- β is linearly independent, $span(\gamma) = V$, $|\beta| \leq |\gamma|$ by Theorem 1.10.
- So, γ is linearly independent and $span(\beta) = V$. Again, by Theorem 1.10, $|\gamma| \leq |\beta|$.

□

Definition 9 A vector space is called *finite-dimensional* if it has a finite basis. The number of vectors in a basis, is called the *dimension* of V, notated $dim(V)$. A vector space which is not finite-dimensional is called *infinite-dimensional*.

Corollary 14 Suppose $dim(V) = n$.

(a) If S is finite and $span(S) = V$, then $n \leq |V|$. If $|S| = n$, then S is a basis.

Proof. Let S be finite and $span(S) = V$. Let β be a basis for V. Then, β is linearly independent and $|\beta| = n$. By Theorem 1.10, $|S| \geq |\beta| = n$. Suppose $|S| = n$. Then S contains a subset T such that T is linearly independent and $span(T) = V$. Consequently, T is a basis fr V. Thus, $|T| = dim(V) = n$, $T \subseteq S$, $|T| = n$. Therefore, $S = T$, which implies S is a basis. □

(b) If $|S| = n$ and S is linearly independent, then S is a basis.

Proof. Suppose L is linearly independent and $|L| = dim(V)$. Let β be a basis for V. Then $|L| \leq |\beta|$, in addition, there exists $H \subseteq \beta$ such that $span(L \cup H) = V$ and $|H| = |\beta| - |L| = dim(V) - dim(V) = 0$. Thus, $H = \emptyset$. Thus $span(L) = V$. □

(c) Every linearly independent set can be extended to a basis.

Proof. Let L be linearly independent. Suppose $|L| < n$. Let β be a basis. Then there exists $H \subseteq \beta$ such that $span(L \cup H) = V$ and $|H| = n - |L|$. So, $|L \cup H| \leq n$. As before, $L \cup H$ contains an independent subset T such that $span(T) = V$. Then T is a basis and so $|T| = n$. Therefore, $T = L \cup H$. Thus $L \cup H$ is a basis. □

Example:

(1) $\mathbb{F}^n$, $dim(\mathbb{F}^n) = n$.

(2) $V = M_{m\times n}(\mathbb{F})$, $dim(V) = mn$.

(3) $V = \{A \in M_{n\times n} : A \text{ is symmetric}\}$, $dim(V) = \frac{n(n+1)}{2}$.

Theorem 1.11. Let W be a subspace of a finite-dimensional space V. Then W is finite-dimensional and $dim(W) \leq dim(V)$. Moreover, if $dim(W) = dim(V)$, then $W = V$.

1.7 Maximal linearly independent subsets

Definition 10 A collection $\mathcal{C}$ of sets is called a *chain* if for every $A, B \in \mathcal{C}$, $A \subseteq B$ or $B \subseteq A$.

Maximal Principle: Let $\mathcal{F}$ be a family of sets. If for every chain $\mathcal{C}$ in $\mathcal{F}$ there is a set in $\mathcal{F}$ which contains all members of $\mathcal{C}$, then $\mathcal{F}$ contains a maximal element.

Theorem 1.12. Every vector space has a basis.

Proof. (Outline)

- Start with an arbitrary (finite) linearly independent set S in V and consider the family $\mathcal{F}$ of all independent sets contains S. Argue that Maximal Principle applies and take the element β in $\mathcal{F}$.
- β generates V.

Cauchy's functional equation:

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

What type of functions can f be?

(1) $f : \mathbb{Q} \to \mathbb{Q}$ where $f(x) = \alpha \cdot x$ and $\alpha = f(1)$.

(2) $f : \mathbb{R} \to \mathbb{R}$ allows for other fairly exotic functions.

For example, $\mathbb{R}$ is a vector space over $\mathbb{Q}$. Let H be a basis of this vector space, commonly called Hamel basis. Then for every element $x \in \mathbb{R}$ there exists unique $h_1, \dots, h_n \in H$ and unique scalars $c_1, \dots, c_n \in \mathbb{Q}$ with $c_1, \dots, c_n \neq 0$ such that $x = \sum_{i=1}^n c_i h_i$. Then, for any $g : H \to \mathbb{R}$, we can extend g to $\overline{g} : \mathbb{R} \to \mathbb{R}$ defined by

$$\overline{g}(x) = \sum_{i=1}^n c_i g(h_i).$$

So,

$$x + y = \sum_{i=1}^n d_i h_i + \sum_{i=1}^n a_i h_i = \sum_{i=1}^n c_i h_i.$$

2 Linear Transformations and Matrices

2.1 Linear transformations, null spaces, and ranges

Definition 1 A function $T : V \to W$ is called a *linear transformation* from V to W if for all $x, y \in V$ and $c \in \mathbb{F}$ the following hold.

- $T(x + y) = T(x) + T(y)$
- $T(cx) = cT(x)$

Observations:

- T is linear if and only if $x_1, \dots, x_n \in V$, $a_1, \dots, a_n \in \mathbb{F}$

$$T\left(\sum_{i=1}^{n} a_i x_i\right) = \sum_{i=1}^{n} a_i T(x_i).$$

- T is linear if and only if $T(cx + y) = cT(x) + T(y)$ for $x, y \in V$, $c \in \mathbb{F}$.

Example:

(1) Define $T : \mathbb{R}^2 \to \mathbb{R}^2$ to be $T(a_1, a_2) = (2a_1 + a_2, a_1)$. Then

$$\begin{aligned} T((a_1, a_2) + (b_1, b_2)) &= T(a_1 + b_1, a_2 + b_2) \\ &= (2(a_1 + b_1) + a_2 + b_2, a_1 + b_1) \\ &= (2a_1 + a_2, a_1) + (2b_1 + b_2, b_1) \\ &= T(a_1, a_2) + T(b_1, b_2). \end{aligned}$$

It's also easy to show,

$$T(c(a_1, a_2)) = cT(a_1, a_2).$$

(2) Let $T_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ where $T_\theta(a_1, a_2)$ is the vector obtained by (a_1, a_2) by the angle θ.

(3) Let $V = \mathcal{C}(\mathbb{R})$, and $a, b \in \mathbb{R}$, with $a < b$. Let $T : V \to \mathbb{R}$, where

$$T(f) = \int_a^b f(t)dt.$$

Then, $T(f + g) = T(f) + T(g)$. Also, $T(cf) = cT(f)$.

Definition 2 Let $T : V \to W$ be linear.

- The *null space* (kernel) $N(T) = \{x \in V : T(x) = 0\}$

- The *range* (image) $R(T) = \{T(x) : x \in V\}$

Theorem 2.1. Let $T : V \to W$ be linear. Then $N(T)$ and $R(T)$ are subspaces of V and W.

Proof.

(1) We have $0_V \in N(T)$ because $T(0_V) = 0_W$.

(2) Suppose $x, y \in N(T)$. Then $T(x) = 0_W$, $T(y) = 0_W$. Thus, $T(x + y) = T(x) + T(y) = 0_W + 0_W = 0_W$. Thus $x + y \in N(T)$.

(3) Suppose $x \in N(T)$ and $c \in \mathbb{F}$. then $T(x) = 0_W$ and so $T(cx) = cT(x) = 0_W$. Thus, $cx \in N(T)$.

Therefore $N(T)$ is a subspace of V. $R(T)$ can be shown to be a subspace of V in a similar manner. □

Theorem 2.2. Let $T : V \to W$ be linear and let $\beta = \{v_1, \ldots, v_n\}$ be a basis for V. Then $R(T) = span(T(\beta)) = span(\{T(v_1), \ldots, T(v_n)\})$.

Proof.

(1) Let $w \in R(T)$. Then $w = T(v)$ for some $v \in V$. Then $v = \sum_{i=1}^{n} c_i v_i$ for some $c_1, \ldots, c_n \in \mathbb{F}$. Thus, $T(v) = \sum_{i=1}^{n} c_i T(v_i)$. Therefore, $w = T(v) \in span(T(\beta))$.

(2) Let $w \in span(T(\beta))$. Then $w = \sum_{i=1}^{n} c_i T(v_i)$ for some $c_1, \ldots, c_n \in \mathbb{F}$. Thus $w = T\left(\sum_{i=1}^{n} c_i v_i\right)$ and $\sum_{i=1}^{n} c_i v_i \in V$. Thus $w \in R(T)$.

□

- $nullity(T) = dim(N(T))$
- $rank(T) = dim(R(T))$

Theorem 2.3. (Dimension Theorem) Let $T : V \to W$ be linear. If V is finite-dimensional, then

$$nullity(T) + rank(T) = dim(T).$$

Proof. (Outline)

- Start with a basis for $N(T)$, $\{v_1, \ldots, v_k\}$ and extend it to a basis of V, $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$.
- Prove that $\{T(v_{k+1}), \ldots, T(v_n)\}$ is a basis for $R(T)$.

Proof. Let $\{v_1, \ldots, v_k\}$ be a basis for $N(T)$. Extend this basis to a basis β for V, say $\beta = \{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$. Note, $k = dim(N(T))$ and $n = dim(V)$. We claim that $\{T(v_{k+1}), \ldots, T(v_n)\}$ is a basis for $R(T)$.

(1) Clearly, $span(\{T(v_{k+1}), \ldots, T(v_n)\}) \subseteq R(T)$. Let $w \in R(T)$. Then $w = T(v)$ for some $v \in V$ and $v = \sum_{i=1}^n c_i v_i$ for some $c_1, \ldots, c_n \in \mathbb{F}$. Then $w = T(v) = \sum_{i=1}^n c_i T(v_i) = \sum_{i=k+1}^n c_i T(v_i)$ since $T(v_i) = 0$ for $i \leq k$. Therefore, $w \in span(\{T(v_{k+1}), \ldots, T(v_n)\})$. So, $span(\{T(v_{k+1}), \ldots, T(v_n)\}) = R(T)$.

(2) We'll show $\{T(v_{k+1}), \ldots, T(v_n)\}$. is linearly independent. Suppose $\sum_{i=k+1}^n c_i T(v_i) = 0$. Then, $T\left(\sum_{k+1}^n c_i v_i\right) = 0$. Thus, $\sum_{k+1}^n c_i v_i \in N(T)$. So, $\sum_{k+1}^n c_i v_i = \sum_{i=1}^k d_i v_i$ for some $d_1, \ldots, d_k \in \mathbb{F}$. Therefore, $\sum_{k+1}^n c_i v_i - \sum_{i=1}^k d_i v_i = 0$. Since β is linearly independent, $c_{k+1} = \cdots = c_n = 0$. In addition, $d_1 = \cdots = d_k = 0$. Thus, $\{T(v_{k+1}), \ldots, T(v_n)\}$ is linearly independent.

□

Theorem 2.4. Let $T : V \to W$ be linear. Then T is injective if and only if $N(T) = \{0\}$.

Proof.
($\Longrightarrow$): Suppose $T : V \to W$ is injective. If $T(x) = 0$ then since $T(0) = 0$, we have $T(x) = T(0)$ and so $x = 0$.
($\Longleftarrow$): Suppose $N(T) = \{0\}$. If $T(x) = T(y)$, then $T(x) - T(y) = 0$. Thus, $T(x - y) = 0$. Thus, $x - y \in N(T)$, which implies $x - y = 0$ and thus $x = y$. □

Theorem 2.5. Let V, W be finite-dimensional vector spaces such that $dim(V) = dim(W)$ and let $T : V \to W$ be linear. Then the following are equivalent:

(a) T is injective;

(b) T is surjective;

(c) $rank(T) = dim(V) = dim(W)$.

Proof. Note, T being injective is equivalent to $N(T) = \{0\}$, which is equivalent to $nullity(T) = 0$. By the dimension theorem, $rank(T) = dim(V)$. So, $rank(T) = dim(W)$, which is equivalent to $dim(R(T)) = dim(W)$. This is equivalent to $R(T) = W$ since $R(T) \subseteq W$. Thus, T is surjective. □

Theorem 2.6. Suppose $\{v_1, \ldots, v_n\}$ is a basis for V. For $w_1, \ldots, w_n \in W$ there exists exactly one linear transformation $T : V \to W$ such that $T(v_i) = w_i$ for every i.

Proof. (Outline)

- For $x \in V$ we can write $x = \sum_{i=1}^{n} a_i v_i$ uniquely.
- Let $T : V \to W$ be $T(x) = \sum_{i=1}^{n} a_i w_i$.

Proof. Let $\{v_1, \ldots, v_n\}$ be a basis for V and $w_1, \ldots, w_n \in W$. Then there exists unique $T : V \to W$ defined by $T(v_i) = w_i$.

(1) Let $x \in V$. Then x can be uniquely written as $x = \sum_{i=1}^{n} a_i v_i$ where $a_i \in \mathbb{F}$. Let $T(x) \coloneqq \sum_{i=1}^{n} a_i w_i$. $T : V \to W$ is well-defined, and thus a function.

(2) Let T be linear and $u, v \in V$. Let $c \in \mathbb{F}$. We will show $T(cu + v) = cT(u) + T(v)$. Then, $u = \sum_{i=1}^{n} a_i v_i$ and $v = \sum_{i=1}^{n} b_i v_i$ for unique $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{F}$. Then $cu + v = \sum_{i=1}^{n} (ca_i + b_i) v_i$. So,

$$\begin{aligned} T(cu+v) &= \sum_{i=1}^{n} (ca_i + b_i) w_i \\ &= c \sum_{i=1}^{n} a_i w_i + \sum_{i=1}^{n} b_i w_i \\ &= cT(u) + T(v). \end{aligned}$$

(3) Suppose $U : V \to W$ is linear and $U(v_i) = w_i$. Let $x \in V$. Then $x = \sum_{i=1}^{n} a_i v_i$. Then

$$\begin{aligned} U(x) &= U\left(\sum_{i=1}^{n} a_i v_i \right) \\ &= \sum_{i=1}^{n} a_i U(v_i) \\ &= \sum_{i=1}^{n} a_i w_i \\ &= T(x). \end{aligned}$$

(4) Note, $T(v_i) = w_i$ because $v_i = 1 \cdot v_i$. Thus, $T(v_i) = 1 \cdot w_i = w_i$.

□

Corollary 7 Let $\{v_1, \ldots, v_n\}$ be a basis of V. If $U, T : V \to W$ are linear and $T(v_i) = U(v_i)$, then $T = U$.

2.2 The matrix representation of a linear transformation

Definition 3 Let V be a finite-dimensional vector space. An *ordered basis* for V is a basis equipped with an ordering.

Example: Let $\beta = \left\{ e_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}, e_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}, e_3 = \begin{pmatrix}0\\0\\1\end{pmatrix} \right\}$. Let $x = \begin{pmatrix}5\\6\\7\end{pmatrix} = 5e_1 + 6e_2 + 7e_3$.
Then $\left[x\right]_\beta = \begin{pmatrix}5\\6\\7\end{pmatrix}$.

Definition 4 Let $\beta = \{u_1, \ldots, u_n\}$ be an ordered basis for V. Then for every $x \in V$, $x = \sum a_i u_i$ and $a_1, \ldots, a_n$ are unique. The coordinate vector of x relative to β, $\left[x\right]_\beta = (a_1, \ldots, a_n)^T$.

Let $T : V \to W$, $\beta = \{v_1, \ldots, v_n\}$, $\gamma = \{w_1, \ldots, w_m\}$ be ordered bases for V and W. We have

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

Then $A = \left[a_{ij}\right]$ is called the matrix representation of T in the ordered bases β and γ and we write

$$A = \left[T\right]_\beta^\gamma.$$

If $V = W$ and $\beta = \gamma$, we say $A = \left[T\right]_\beta$.

Observations:

- The jth column of A is $\left[T(v_j)\right]_\gamma$.
- If $T, U : V \to W$ and $\left[U\right]_\beta^\gamma = \left[T\right]_\beta^\gamma$, then $T = U$.

Example: Let $T : \mathbb{R}^2 \to \mathbb{R}^2$, $\beta = \{(1,0),(0,1)\}$ and $\gamma = \{(1,1),(1,-1)\}$. Let $T((1,0)) = (1,0)$ and $T((0,1)) = (1,1)$. Find $\left[T\right]_\beta^\gamma$.

We can see $T((1,0)) = (1,0) = \frac{1}{2}(1,1) + \frac{1}{2}(1,-1)$. Also, $T((0,1)) = (1,1) = 1(1,1) + 0(1,-1)$. Therefore, $\left[T\right]_\beta^\gamma = \begin{pmatrix}\frac{1}{2} & 1\\ \frac{1}{2} & 0\end{pmatrix}$.

Theorem 2.7. Let $T, U : V \to W$ are linear and let $a \in \mathbb{F}$. Then,

- $aT + U$ is linear.

- The set of all linear transformations from V to W (with addition of functions and scalar multiplication) forms a vector space over F.

We notate $\mathcal{L}(V, W)$ as the vector space of all linear transformations from V to W. Also, $\mathcal{L}(V) = \mathcal{L}(V, V)$.

Theorem 2.8. Let $T, U : V \to W$ be linear. Then,

- $\left[T + U\right]_\beta^\gamma = \left[T\right]_\beta^\gamma + \left[U\right]_\beta^\gamma$
- $\left[aT\right]_\beta^\gamma = a\left[T\right]_\beta^\gamma$.

2.3 Composition of linear transformations and matrix multiplication

Theorem 2.9. Let $T : V \to W$, $U : W \to Z$ be linear. Then $UT : V \to Z$ is linear.

Proof. Let $T : V \to W$, $U : W \to Z$ be linear. Then,

$$\begin{aligned} UT(au + v) &= U(T(au + v)) \\ &= U(aT(u) + T(v)) \\ &= aU(T(u)) + U(T(v)) \\ &= aUT(u) + UT(v). \end{aligned}$$

□

Theorem 2.10. Let $T, U_1, U_2 \in \mathcal{L}(V)$. Then

- $T(U_1 + U_2) = TU_1 + TU_2$ and $(U_1 + U_2)T = U_1T + U_2T$
- $T(U_1U_2) = (TU_1)U_2$
- $TI = IT = T$
- $a(U_1U_2) = (aU_1)U_2 = U_1(aU_2)$

Definition 5 Let A be an $m \times n$ matrix, B be an $n \times p$ matrix. We define AB to be the $m \times p$ matrix such that

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj}.$$

Note: $(AB)^t = B^tA^t$.

Theorem 2.11. Let $T : V \to W$. $U : W \to Z$ be linear and let α, β, γ be ordered bases in V, W, Z. Then

$$\left[UT\right]_{\alpha}^{\gamma} = \left[U\right]_{\beta}^{\gamma} \left[T\right]_{\alpha}^{\beta}.$$

Proof. (Outline)

- $\alpha = \{v_1, \ldots, v_m\}$, $\beta = \{w_1, \ldots, w_n\}$, $\gamma = \{z_1, \ldots, z_p\}$.
- $A = \left[U\right]_{\beta}^{\gamma}$, $B = \left[T\right]_{\alpha}^{\beta}$
- $U(T(v_j)) = U\left(\sum_{k=1}^{n} B_{kj} w_k\right) = \sum_{k=1}^{n} B_{kj} U(w_k) = \sum_{k=1}^{n} B_{kj} \sum_{i=1}^{p} A_{ik} z_i = \sum_{i=1}^{p} C_{ij} z_i$
- Thus, by definition, the i, jth entry in $\left[UT\right]_{\alpha}^{\gamma}$ is $C_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj}$.

Proof. Let $\alpha = \{v_1, \ldots, v_n\}, \beta = \{w_1, \ldots, w_m\}$ and $\gamma = \{z_1, \ldots, z_p\}$. Let $A = \left[U\right]_{\beta}^{\gamma}$ and $B = \left[T\right]_{\alpha}^{\beta}$. Consider $\left[UT\right]_{\alpha}^{\gamma}$. Then

$$\begin{aligned}
(UT)(v_j) &= U(T(v_j)) \\
&= U\left(\sum_{i=1}^{m} B_{ij} w_i\right) \\
&= \sum_{i=1}^{m} B_{ij} U(w_i) \\
&= \sum_{i=1}^{m} B_{ij} \cdot \sum_{k=1}^{p} A_{ki} z_k \\
&= \sum_{k=1}^{p} \left(\sum_{i=1}^{m} A_{ki} B_{ij}\right) z_k.
\end{aligned}$$

If $C = \left[UT\right]_{\alpha}^{\gamma}$, then

$$C_{kj} = \sum_{i=1}^{m} A_{ki} B_{ij}.$$

□

Example: Let $\alpha = \{1, x, x^2\}$ and $\beta = \{1, x, x^2, x^3\}$ be standard bases for $P_2(\mathbb{R})$ and $P_3(\mathbb{R})$. Let $U : P_3(\mathbb{R}) \to P_2(\mathbb{R})$ and $T : P_2(\mathbb{R}) \to P_3(\mathbb{R})$ defined by $U(f(x)) = f'(x)$ and $T(f(x)) = \int_0^x f(t)dt$. From calculus, $UT = I$. We can see

$$\begin{aligned}
U(1) &= 0 = 0 \cdot 1 + 0 \cdot x + 0 \cdot x^2 \\
U(x) &= 1 = 1 \cdot 1 + 0 \cdot x + 0 \cdot x^2 \\
U(x^2) &= 2x = 0 \cdot 1 + 2 \cdot x + 0 \cdot x^2 \\
U(x^3) &= 3x^2 = 0 \cdot 1 + 0 \cdot x + 3 \cdot x^2.
\end{aligned}$$

Also,

$$\begin{aligned} T(1) &= x = 0\cdot 1 + 1\cdot x + 0\cdot x^2 + 0\cdot x^3 \\ T(x) &= \frac{1}{2}x^2 = 0\cdot 1 + 0\cdot x + \frac{1}{2}x^2 + 0\cdot x^3 \\ T(x^2) &= \frac{1}{3}x^3 = 0\cdot 1 + 0\cdot x + 0\cdot x^2 + \frac{1}{3}x^3. \end{aligned}$$

Thus,

$$\begin{aligned} \left[UT\right]_\alpha^\alpha &= \left[U\right]_\beta^\alpha \left[T\right]_\alpha^\beta \\ &= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{3} \end{pmatrix} \\ &= I. \end{aligned}$$

Theorem 2.12. Let A be an $m\times n$ matrix, B and C be $n\times p$ matrices, D, E be $q\times m$ matrices. Then

- $A(B+C) = AB + AC$, $(D+E)A = DA + EA$
- $a(AB) = (aA)B = A(aB)$
- $I_m A = A = AI_n$
- If V is n-dimensional with ordered basis β, then $\left[I_V\right]_\beta = I_n$

Theorem 2.13. Let A be an $m\times n$ matrix, B be an $n\times p$ matrix. Let u_j, v_j denote the jth columns of AB and B. Then

(a) $u_j = Av_j$

(b) $v_j = Be_j$

Theorem 2.14. Let V, W be finite-dimensional vector spaces with ordered bases β and γ and let $T : V \to W$ be linear. Then for $u \in V$

$$\left[T(u)\right]_\gamma = \left[T\right]_\beta^\gamma \left[u\right]_\beta .$$

Proof. Let V, W be finite-dimensional vector spaces with ordered bases β and γ and let $T : V \to W$ be linear. Fix $u \in V$. Let $f : \mathbb{R} \to V$ and $g : \mathbb{R} \to W$ where $f(a) = au$

and $g(a) = aT(u)$. Let $\alpha = \{1\}$ be the standard basis for $\mathbb{R}$. Note that, g and f are linear transformations. Then,

$$\begin{aligned}
\left[T(u)\right]_\gamma &= \left[g(1)\right]_\gamma \\
&= \left[g\right]_\alpha^\gamma \\
&= \left[Tf\right]_\alpha^\gamma \\
&= \left[T\right]_\beta^\gamma \left[f\right]_\alpha^\beta \\
&= \left[T\right]_\beta^\gamma \left[f(1)\right]_\beta \\
&= \left[T\right]_\beta^\gamma \left[u\right]_\beta .
\end{aligned}$$

□

Let $L_A : \mathbb{F}^n \to \mathbb{F}^m$ be given by $L_A(x) = Ax$ where A is an $m \times n$ matrix.

Theorem 2.15. Let A be an $m \times n$ matrix. Then L_A is linear. Moreover, if $B \in M_{m\times n}(\mathbb{F})$ and β and γ are the standard ordered bases of $\mathbb{F}^n$ and $\mathbb{F}^m$, then

(a) $\left[L_A\right]_\beta^\gamma = A$

(b) $L_A = L_B$ if and only if $A = B$

(c) $L_{A+B} = L_A + L_B$, $L_{aA} = aL_A$

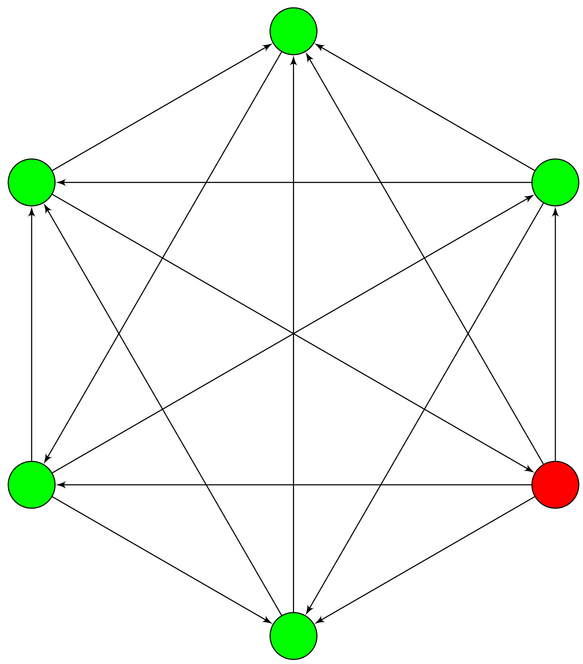
(d) If $T : \mathbb{F}^n \to \mathbb{F}^m$ is linear, then there exists unique matrix C (namely $C = \left[T\right]_\beta^\gamma$) such that $T = L_C$.

(e) If E is an $n \times p$ matrix, then $L_{AE} = L_A L_E$

(f) If $m = n$, $L_{I_n} = I_{\mathbb{F}^n}$.

Theorem 2.16. Let A, B, C be such that $A(BC)$ is defined then $(AB)C = A(BC)$.

Tournaments: There are n players $\{1, \ldots, n\}$ for every $i \neq j$ there is exactly one game between i and j which results in i winning or j winning. Let A be the incidence matrix of a tournament where we put $A_{ij} = 1$ if i wins with j and 0 otherwise. Show that $A^2 + A$ contains a column such that each entry but the diagonal is at least one.



2.4 Invertibility and isomorphisms

Definition 6 Let $T : V \to W$ be linear. A function $U : W \to V$ is called an *inverse* of T if $UT = I_V$, $TU = I_W$. If T has an inverse, then it's called *invertible*.

Note:

- If T is invertible, then the inverse is unique, denoted by T^{-1}.
- $(UT)^{-1} = T^{-1}U^{-1}$
- $(T^{-1})^{-1} = T$
- T is invertible if and only if T is a bijection.
- $T : V \to W$, V, W are finite-dimensional of equal dimensions.
- T is invertible if and only if $rank(T) = dim(v)$.

Theorem 2.17. Let $T : V \to W$ be linear and invertible. Then $T^{-1} : W \to V$ is linear.

Proof. Suppose $T : V \to W$ is linear and invertible. Then $T^{-1} : W \to V$. Let $y_1, y_2 \in W$. Since T is bijective, there exists unique $x_1, x_2 \in V$ such that $T(x_1) = y_1$ and

$T(x_2) = y_2$. Let $c \in \mathbb{F}$. Then

$$\begin{aligned} T^{-1}(cy_1 + y_2) &= T^{-1}(cT(x_1) + T(x_2)) \\ &= T^{-1}(T(cx_1 + x_2)) \\ &= cx_1 + x_2 \\ &= cT^{-1}(y_1) + T^{-1}(y_2). \end{aligned}$$

□

Definition 7 Let A be an $n \times n$ matrix. Then A is *invertible* if there exists an $n \times n$ matrix B such that $AB = BA = I$. Then B is called the inverse of A denoted by A^{-1}.

Lemma 19. Let T be an invertible transformation from V to W. Then V is finite-dimensional if and only if W is. In this case $dim(V) = dim(W)$.

Proof. Let T be an invertible transformation from V to W. Then T must be bijective. Suppose V is finite-dimensional. Let $\beta = \{v_1, \ldots, v_n\}$ be a basis for V. Then $dim(V) = n$. Then $T(\beta) = \{T(v_1), \ldots, T(v_n)\}$ generates W because T is surjective. Let $w \in W$. Then there exists $v \in V$ such that $T(v) = w$. Then $v = \sum_{i=1}^{n} a_i v_i$. Thus, $T(v) = \sum_{i=1}^{n} a_i T(v_i)$. As a result, $dim(W) \leq n = dim(V)$. However, $T^{-1} : W \to V$ is also linear. Then the same argument implies $dim(V) \leq dim(W)$. Therefore, $dim(V) = dim(W)$. □

Theorem 2.18. Let V, W be finite-dimensional with ordered bases β and γ. Let $T : V \to W$ be linear. Then T is invertible if and only if $[T]_{\beta}^{\gamma}$ is invertible. Furthermore $[T^{-1}]_{\gamma}^{\beta} = ([T]_{\beta}^{\gamma})^{-1}$.

Proof. (Outline)

- If T is invertible, then by the lemma $dim(V) = dim(W)$ and the fact that $[T]_{\beta}^{\gamma}$ follows from previous facts and $T^{-1}T = I_V$.
- If $[T]_{\beta}^{\gamma}$ is invertible then it has an inverse B and so there is a transformation $U : W \to V$ with $B = [U]_{\gamma}^{\beta}$. Now check that $UT = I_V$.

Proof. Suppose T is invertible. Then by the lemma $dim(V) = dim(W) = n$, and in addition, there exists $U : W \to V$ such that $TU = I_W$ and $UT = I_V$. Let β, γ be bases for V, W respectively. Then

$$I = [I_V]_{\beta} = [UT]_{\beta} = [U]_{\gamma}^{\beta} [T]_{\beta}^{\gamma}.$$

In the same way,

$$[I_W]_{\gamma} = [TU]_{\gamma} = [T]_{\beta}^{\gamma} [U]_{\gamma}^{\beta}.$$

Thus, $\left[U\right]_\gamma^\beta = \left(\left[T\right]_\beta^\gamma\right)^{-1}$.

Now, assume $\left[T\right]_\beta^\gamma$ is invertible. Let $A = \left[T\right]_\beta^\gamma$. Then A is an $n \times n$ matrix. Let $\beta = \{v_1, \ldots, v_n\}$ and $\gamma = \{w_1, \ldots, w_n\}$. Since A is invertible, there exists B such that $AB = I_n = BA$. Then there exists unique linear transformation $U : W \to V$ such that $U(w_j) = \sum_{i=1}^n B_{ij} v_i$. Then $\left[U\right]_\gamma^\beta = B$. Thus $\left[TU\right]_\gamma = \left[T\right]_\beta^\gamma \left[U\right]_\gamma^\beta = A \cdot B = I_n = \left[I_W\right]_\gamma$. Also, $\left[UT\right]_\beta = B \cdot A = I_n = \left[I_V\right]_\beta$. Thus $TU = I_W$ and $UT = I_V$. $\square$

Definition 8 Vector space V is isomorphic to W if there is an invertible linear transformation $T : V \to W$.

Example: Let $T : P_3(\mathbb{R}) \to M_{2\times 2}(\mathbb{R})$ be defined by

$$T(f) = \begin{pmatrix} f(1) & f(2) \\ f(3) & f(4) \end{pmatrix}.$$

Then

(1) T is linear.

$$T(f+g) = T(f) + T(g)$$
$$T(cf) = cT(f)$$

(2) T is injective. (This is because $N(T) = \{0\}$.)

(3) $dim(P_3(\mathbb{R})) = 4$ and $dim(M_{2\times 2}(\mathbb{R})) = 4$

(4) T is surjective

(5) T is bijective

(6) $P_3(\mathbb{R}) \cong M_{2\times 2}(\mathbb{R})$

Theorem 2.19. Let V, W be finite-dimensional over F. Then V is isomorphic to W if and only if $dim(V) = dim(W)$.

Proof.
($\Longrightarrow$): Suppose $V \cong W$. By the lemma, $dim(V) = dim(W)$.

($\Longleftarrow$): Suppose $dim(V) = dim(W)$. Let $\beta = \{v_1, \ldots, v_n\}$ be a basis for V and let $\gamma = \{w_1, \ldots, w_n\}$ be a basis for W. Then there exists a unique linear transformation $T : V \to W$ such that $T(v_i) = w_i$. Then T is surjective. Since $dim(V) = dim(W)$, T is injective. Thus T is invertible. Therefore, $V \cong W$. $\square$

Theorem 2.20. Let V, W be finite-dimensional over F of dimensions n and m. Let β, γ be ordered bases for V and W. Then $\Phi : \mathcal{L}(V, W) \to M_{m\times n}(\mathbb{F})$ given by $\Phi(T) = \left[T\right]_\beta^\gamma$ for $T \in \mathcal{L}(V, W)$ is an isomorphism.

Proof. Let $\Phi(T) = \left[T\right]_\beta^\gamma$.

(1) Let $\phi : \mathcal{L}(V, W) \to M_{m\times n}(\mathbb{F})$. Then Φ is linear.

$$\begin{aligned}\Phi(aT + U) &= \left[aT + U\right]_\beta^\gamma \\ &= \left[aT\right]_\beta^\gamma + \left[U\right]_\beta^\gamma \\ &= a\left[T\right]_\beta^\gamma + \left[U\right]_\beta^\gamma\end{aligned}$$

(2) For every $A \in M_{m\times n}(\mathbb{F})$ there exists unique transformation T such that $\Phi(T) = A = \left[A_{ij}\right]$. Let $\beta = \{v_1, \ldots, v_n\}$ and $\gamma = \{w_1, \ldots, w_m\}$. Then there exists unique transformation $T : V \to W$ such that

$$T(v_j) = \sum_{i=1}^{n} A_{ij} w_i,$$

for $j = 1, \ldots, n$ and $i = 1, \ldots, m$. Thus

$$\left[T\right]_\beta^\gamma = A.$$

Thus $\Phi(T) = \left[T\right]_\beta^\gamma = A$.

□

Definition 9 Let β be an ordered basis for an n-dimensional vector space V over F. The *standard representation of* V *with respect to* β is the function $\phi_\beta : V \to \mathbb{F}^n$ defined as $\phi_\beta(x) = \left[x\right]_\beta$.

Theorem 2.21. Let V be a finite-dimensional vector space with ordered basis β. Then ϕ_β is an isomorphism.

Note: For vector fields V and W with basis β and γ, respectively, we have the following schematic representation:

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "\phi_\beta"'] & W \arrow[d, "\phi_\gamma"] \\ \mathbb{F}^n \arrow[r, "L_A"] & \mathbb{F}^m \end{tikzcd}$$

Where $L_A(x) = Ax$ and $A = \left[T\right]_\beta^\gamma$, we have

$$L_A\phi_\beta = \phi_\gamma T.$$

That is,

$$\left[T\right]_\beta^\gamma \left[u\right]_\beta = \left[T(u)\right]_\gamma.$$

2.5 The change of coordinate matrix

Theorem 2.22. Let β, β' be two ordered bases for a finite-dimensional vector space V and let $Q = \left[I_V\right]_{\beta'}^{\beta}$. Then

(a) Q is invertible.

(b) For any $v \in V$, $\left[v\right]_{\beta} = Q\left[v\right]_{\beta'}$

Proof.

(a) We know $\left[I_V\right]_{\beta'}^{\beta}$ is invertible because $I_V : V \to V$ is invertible. So, $I_V^{-1} = I_V$.

(b) We have $\left[u\right]_{\beta} = Q \cdot \left[u\right]_{\beta'}$. So, $\left[u\right]_{\beta} = \left[I_V(u)\right]_{\beta} = \left[I_V\right]_{\beta'}^{\beta}\left[u\right]_{\beta'}$.

$\square$

Example: Let $\beta = \left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\end{pmatrix}\right\}$ and $\beta' = \left\{\begin{pmatrix}2\\4\end{pmatrix}, \begin{pmatrix}3\\1\end{pmatrix}\right\}$. Then

$$
\begin{aligned}
\begin{pmatrix}2\\4\end{pmatrix} &= 3\begin{pmatrix}1\\1\end{pmatrix} - \begin{pmatrix}1\\-1\end{pmatrix}, \\
\begin{pmatrix}3\\1\end{pmatrix} &= 2\begin{pmatrix}1\\1\end{pmatrix} + \begin{pmatrix}1\\-1\end{pmatrix}, \\
\left[I_V\right]_{\beta'}^{\beta} &= \begin{pmatrix}3 & 2\\-1 & 1\end{pmatrix}, \\
\left[\begin{pmatrix}2\\4\end{pmatrix}\right]_{\beta} &= Q\left[\begin{pmatrix}2\\4\end{pmatrix}\right]_{\beta'} \\
&= Q\begin{pmatrix}1\\0\end{pmatrix} \\
&= \begin{pmatrix}3\\-1\end{pmatrix}.
\end{aligned}
$$

Q is called the change of coordinate matrix. A linear operator on V is the linear transformation from V to V.

Theorem 2.23. Let T be a linear operator on a finite-dimensional vector space V. Let β, β' be ordered bases for V. Suppose $Q = \left[I_V\right]_{\beta'}^{\beta}$. Then

$$\left[T\right]_{\beta'} = Q^{-1}\left[T\right]_{\beta} Q.$$

Proof. Suppose $Q = \left[I_V\right]_{\beta'}^{\beta}$. Note that $I_V Q = Q = Q I_V$. Then,

$$\begin{aligned} Q\left[T\right]_{\beta'} &= \left[I_V\right]_{\beta'}^{\beta}\left[T\right]_{\beta'} \\ &= \left[I_V T\right]_{\beta'}^{\beta} \\ &= \left[T I_V\right]_{\beta'}^{\beta} \\ &= \left[T\right]_{\beta}\left[I_V\right]_{\beta'}^{\beta} \\ &= \left[T\right]_{\beta}\cdot Q. \end{aligned}$$

So, $Q^{-1}Q\left[T\right]_{\beta'} = Q^{-1}\left[T\right]_{\beta}Q$. Therefore, $\left[T\right]_{\beta'} = Q^{-1}\left[T\right]_{\beta}Q$. □

Corollary 26 Let $A \in M_{n\times n}(\mathbb{F})$ and let $\gamma = \{u_1, \ldots, u_n\}$ be an ordered basis for $\mathbb{F}^n$. Then $\left[L_A\right]_{\gamma} = Q^{-1}AQ$ where Q is the matrix with the jth column equal to u_j.

Note: We say B **is similar to** A if there exists an invertible matrix C such that

$$B = C^{-1}AC.$$

Example: Let $A = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 1 \\ -1 & 0 & 1 \end{pmatrix}$. Find A^{100}.

Solution. Let $\gamma = \left\{ \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$.

(1) Find $\left[L_A\right]_{\gamma}$.

$$\begin{aligned} L_A\left(\begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}\right) &= A\begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 1 \\ -1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}, \\ L_A\left(\begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}\right) &= A\begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 1 \\ -1 & 0 & 1 \end{pmatrix}\begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \\ 2 \end{pmatrix}, \\ L_A\left(\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}\right) &= A\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 1 \\ -1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}. \end{aligned}$$

Thus

$$\left[L_A\right]_{\gamma} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

(2) Note, $Q = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ and $Q^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$. Then $\left[L_A\right]_\gamma = Q^{-1}AQ$. So, $A = Q\left[L_A\right]_\gamma Q^{-1}$. Then we have

$$\begin{aligned} A^{100} &= \left(Q\left[L_A\right]_\gamma Q^{-1}\right)^{100} \\ &= Q\left[L_A\right]_\gamma Q^{-1}Q\left[L_A\right]_\gamma Q^{-1}\dots Q\left[L_A\right]_\gamma Q^{-1} \\ &= Q\left[L_A\right]_\gamma^{100} Q^{-1} \\ &= Q\begin{pmatrix} 1^{100} & 0 & 0 \\ 0 & 2^{100} & 0 \\ 0 & 0 & 2^{100} \end{pmatrix} Q^{-1}. \end{aligned}$$

2.6 Dual spaces

- Linear functional on V – linear transformation from V to F.
- $V^* = \mathcal{L}(V, F)$
- $V^{**} = (V^*)^*$

$$dim(V^*) = dim(V)$$

Let $\beta = \{x_1, \dots, x_n\}$ for $v \in V$ let $\left[v\right]_\beta = (a_1, \dots, a_n)^T$. Define

$$f_i(v) = a_i.$$

Example:

(1) Let $V =$ continuous functions $f : [0, 2\pi] \to \mathbb{R}$. Let $g \in V$. Define $h : V \to \mathbb{R}$ by

$$h(x) = \frac{1}{2\pi}\int_0^{2\pi} x(t)g(t)dt.$$

Note, h is linear. If $g(t) = \sin(nt)$ or $g(t) = \cos(nt)$, then $h(x)$ is called the nth Fourier coefficient of x.

(2) Let $V = M_{n\times n}(\mathbb{F})$ and $f : V \to \mathbb{F}$ where $f(A) = tr(A)$.

Theorem 2.24. Let V be a finite-dimensional vector space with ordered basis $\beta = \{x_1, \dots, x_n\}$ and let $\beta^* = \{f_1, \dots, f_n\}$. Then β^* is an ordered basis for V^* and for $f \in V^*$ where

$$f = \sum_{i=1}^{n} f(x_i)f_i.$$

Note, $f_i : V \to \mathbb{F}$ is defined as $f_i(x_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{else} \end{cases}$.

Proof. (Outline)

- Enough to show $f = \sum f(x_i) f_i$.
- Let $F \coloneqq \sum f(x_i) f_i$. Then $F(x_j) = f(x_j)$ for every j.

Proof. Let V be a finite-dimensional vector space with ordered basis $\beta = \{x_1, \dots, x_n\}$ and let $\beta^* = \{f_1, \dots, f_n\} \subseteq V^*$ where $n = dim(V) = dim(V^*)$. Since $|\beta^*| = n = dim(V^*)$, it is enough to show that β^* generates V^*. To that end, we will argue that for $f \in V^*$,

$$f = \sum_{i=1}^{n} f(x_i) f_i.$$

Let $g = \sum_{i=1}^{n} f(x_i) f_i$. Then

$$\begin{aligned} g(x_j) &= \left(\sum_{i=1}^{n} f(x_i) f_i \right)(x_j) \\ &= \sum_{i=1}^{n} f(x_i) f_i(x_j) \\ &= \sum_{i=1}^{n} f(x_i) \delta_{ij} \\ &= f(x_j). \end{aligned}$$

Thus, $g(x_j) = f(x_j)$ for every $x_j \in \beta$. Therefore $g = f$. □

Definition 10 An ordered basis $\beta^* = \{f_1, \dots, f_n\}$ for V^* such that $f_i(x_j) = \delta_{ij}$ is called the *dual basis* of $\beta = \{x_1, \dots, x_n\}$.

Theorem 2.25. Let V, W be finite-dimensional vector spaces over $\mathbb{F}$ with ordered bases β and γ. Let $T : V \to W$ be linear. Then $T^t : W^* \to V^*$ given by $T^t(g) = gT$ is linear and

$$[T^t]_{\gamma^*}^{\beta^*} = ([T]_{\beta}^{\gamma})^t.$$

Proof. (Outline)

- It's easy to see that T^t is a linear transformation from W^* to V^*.
- Let $\beta = \{x_1, \dots, x_n\}$, $\gamma = \{y_1, \dots, y_m\}$, $\beta^* = \{f_1, \dots, f_n\}$, $\gamma^* = \{g_1, \dots, g_m\}$, $A = [T]_{\beta}^{\gamma}$.

- The jth column of $\left[T^t\right]_{\gamma^*}^{\beta^*}$ is $T^t(g_j)$ which is

$$\sum_{k=1}^{n}(g_jY)(x_k)f_k.$$

- Thus the i,j-th entry is $(T^t(g_j))(x_i)$ which is A_{ji}.

Proof. Let $T^t : W^* \to V^*$, $T^t(g) = gT$.

(1) Note that $gT : V \to \mathbb{F}$ and gT is a linear transformation. Thus $T^t(g) \in V^*$.

(2) We have T^t is linear. So,

$$\begin{aligned} T^t(cg+h) &= (cg+h)T \\ &= cgT + hT \\ &= cT^t(g) + T^t(h). \end{aligned}$$

(3) Lastly, $\left[T^t\right]_{\gamma^*}^{\beta^*} = \left(\left[T\right]_{\beta}^{\gamma}\right)^t$. Let $\beta = \{x_1, \ldots, x_n\}$, $\gamma = \{y_1, \ldots y_m\}$, $\beta^* = \{f_1, \ldots, f_n\}$, and $\gamma^* = \{g_1, \ldots, g_m\}$. Let $A = \left[T\right]_{\beta}^{\gamma}$. To obtain the jth column of $\left[T\right]_{\gamma^*}^{\beta^*}$,

$$\begin{aligned} T^t(g_j) &= g_jT \\ &= \sum_{k=1}^{n}(g_jT)x_kf_k. \end{aligned}$$

Thus, the i,jth entry of $\left[T\right]_{\gamma^*}^{\beta^*}$ is

$$\begin{aligned} (g_jT)(x_i) &= g_j(T(x_i)) \\ &= g_j\left(\sum_{k=1}^{m} A_{ki}y_i\right) \\ &= \sum_{k=1}^{m} A_{ki}g_j(y_i) && (g_j(y_i) = \delta_{ij}) \\ &= A_{ji}. \end{aligned}$$

□

For $x \in V$ let $\hat{x} : V^* \to \mathbb{F}$ given by $\hat{x}(f) = f(x)$.

Theorem 2.26. Let V be finite-dimensional and let $\psi : V \to V^{**}$ be given by $\psi(x) = \hat{(x)}$. Then ψ is an isomorphism.

3 Elementary matrix operations and systems of linear equations

3.1 Elementary matrix operations and elementary matrices

Definition 1 Let A be a matrix. Elementary row operations:

- Interchange any two rows of A
- Add a scalar multiple of a row of A to another row
- Multiply any row of A by a non-zero scalar

Note: The same can be done for columns.

Definition 2 An $n \times n$ elementary matrix is a matrix obtained from I_n by an elementary operation. Its type is the type of the operation performed.

Theorem 3.1. Let $A \in M_{m\times n}(\mathbb{F})$ and suppose B is obtained by performing an elementary row (column) operation. Then there exists an $m \times m(n \times n)$ elementary matrix E such that $B = EA(B = AE)$.

Example: Note, $\begin{pmatrix} 1 & -7 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is an elementary matrix.

$$\begin{pmatrix} a-7x & b-7y & c-7z \\ x & y & z \\ u & v & w \end{pmatrix} = \begin{pmatrix} 1 & -7 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Theorem 3.2. Elementary matrices are invertible and the inverse of an elementary matrix is an elementary matrix of the same type.

Example: Let $A = \begin{pmatrix} 1 & -7 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Then

$$\begin{aligned} AA^{-1} &= \begin{pmatrix} 1 & -7 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 7 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

3.2 The rank of a matrix and matrix inverse

Definition 3 Let $A \in M_{m\times n}(\mathbb{F})$. The $rank(A)$ is the rank of $L_A : \mathbb{F}^n \to \mathbb{F}^m$. Also $rank(L_A) = dim(R(L_A))$.

Theorem 3.3. Let $T : V \to W$ be linear and let β, γ be ordered bases for V and W. Then

$$rank(T) = rank\left(\left[T\right]_\beta^\gamma\right).$$

Recall, where V and W are vector spaces with bases β and γ, respectively, and $A = \left[T\right]_\beta^\gamma$, we have

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, leftrightarrow] & W \arrow[d, leftrightarrow] \\ \mathbb{F}^n \arrow[r, "L_A"] & \mathbb{F}^m \end{tikzcd}$$

Corollary 3.4.1 Elementary operations are rank-preserving.

Theorem 3.4. Let A be an $m \times n$ matrix. If P and Q are invertible $m \times m$ and $n \times n$ matrices, then

- $rank(AQ) = rank(A)$
- $rank(PA) = rank(A)$

and so $rank(PAQ) = rank(A)$.

Proof. (Outline)

- $R(L_{AQ}) = R(L_A)$ because $L_Q(\mathbb{F}^n) = \mathbb{F}^n$.
- $dim(L_P(L_A(\mathbb{F}^n))) = dim(L_A(\mathbb{F}^n))$ because $L_P : \mathbb{F}^n \to \mathbb{F}^n$ is an isomorphism.

Proof.

(1) Note,

$$\begin{aligned} rank(AQ) &= rank(L_{AQ}) \\ &= dim(R(L_{AQ})). \end{aligned}$$

So,

$$\begin{aligned} R(L_{AQ}) &= R(L_A L_Q) \\ &= L_A L_Q(\mathbb{F}^n) \\ &= L_A(L_Q(\mathbb{F}^n)) \\ &= L_A(\mathbb{F}^n) && \text{(Since } L_Q(\mathbb{F}^n) = \mathbb{F}^n\text{)} \\ &= R(L_A). \end{aligned}$$

Therefore, $dim(R(L_{AQ})) = dim(R(L_A)) = rank(A)$.

(2) We have to show $rank(PA) = rank(A)$. So,

$$\begin{aligned} rank(PA) &= dim(R(L_{PA})) \\ &= dim(L_{PA}(\mathbb{F}^n)) \\ &= dim(L_P(L_A(\mathbb{F}^n))). \end{aligned}$$

Since $L_P : L_A(\mathbb{F}^n) \to L_P(L_A(\mathbb{F}^n))$, then L_P is an isomorphism. Thus, $dim(L_P(L_A(\mathbb{F}^n))) = dim(L_A(\mathbb{F}^n)) = rank(A)$. Therefore, $rank(PA) = rank(A)$.

□

Theorem 3.5. The rank of a matrix equals the maximum number of its linearly independent columns.

Proof. (Outline)

- $R(L_A) = span(L_A(\{e_1, \ldots, e_n\}))$ and $L_A(e_j)$ is the ith column of A.

Proof. Let $A \in M_{m\times n}(\mathbb{F}^n)$. Then

$$\begin{aligned} rank(A) &= dim(R(L_A)) \\ &= dim(L_A(\mathbb{F}^n). \end{aligned}$$

Let β be the standard basis for $\mathbb{F}^n$. We have $span(\beta) = \mathbb{F}^n$. Therefore,

$$\begin{aligned} R(L_A) &= span(L_A(\beta)) \\ &= span(\{L_A(e_1), \ldots, L_A(e_n)\}. \end{aligned}$$

We have $L_A(e_i) = a_i$ where a_i is the ith column of A. Thus, $R(L_A) = span(\{a_1, \ldots, a_n\}$. Thus, $dim(R(L_A))$ is the maximum number of linearly independent columns. □

Example: Find the rank of

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 0 & 3 \\ 1 & 1 & 1 \end{pmatrix}.$$

Solution.

$$
\begin{aligned}
A &\xrightarrow{\text{Row Op.}} \begin{pmatrix} 1 & 2 & 1 \\ 0 & -2 & 2 \\ 0 & -1 & 0 \end{pmatrix} \\
&\xrightarrow{\text{Col. Op.}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 2 \\ 0 & -1 & 0 \end{pmatrix} \\
&\xrightarrow{\text{Row Op.}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 2 \end{pmatrix} \\
&\xrightarrow{\text{Row Op.}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.
\end{aligned}
$$

Therefore, $rank(A) = 3$.

Theorem 3.6. Let A be an $m \times n$ matrix of rank r. Then $r \leq min\{m, n\}$ and A can be transformed to

$$D = \begin{pmatrix} I_r & 0_1 \\ 0_2 & 0_3 \end{pmatrix}$$

using a finite number of elementary row and column operations.

Proof. (Outline) Induction on m. In the inductive step use row and column operations to reduce to

$$\left(\begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ & & B' & \\ 0 & & & \end{array}\right).$$

Proof. If A is the zero matrix, then $rank(A) = 0$ and $D = A$, thus $r = 0$. Suppose A is non-zero. We will use induction on m.

(Base Step) Let $m = 1$. Then A has one row. Then by applying elementary column operations, we can transform A to $\begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix}$ and so $r = 1$ and $rank(A) = 1$.

(Induction Step) Suppose $n \geq 2$. If $n = 1$, then A can be transformed into $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.

So, $r = 1 = rank(A)$. Let $n \geq 2$. So, there exists A_{ij} such that $A_{ij} \neq 0$ and we can transform A so that A_{ij} is in position (1,1). Therefore, we can transform A to

$$\left(\begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ & & B & \\ 0 & & & \end{array}\right)$$

and $rank(B) = rank(A) - 1 = r - 1$. By the inductive hypothesis, $r - 1 \leq m - 1$ and $r - 1 \leq n - 1$ and B can be transformed to

$$\begin{pmatrix} I_{r-1} & 0_4 \\ 0_5 & 0_6 \end{pmatrix}.$$

Thus, A can be transformed to

$$\begin{pmatrix} I_r & 0_1 \\ 0_2 & 0_3 \end{pmatrix}$$

for some 0_i.

$\square$

Note, if $m = n$ and $rank(A) = n$, then $B = I_n$. The converse of this statement is also true.

Corollary 7 Let A be an $m \times n$ matrix of rank r. Then there exist invertible matrices B and C of sizes $m \times m$ and $n \times n$ such that $D = BAC$.

As a consequence of the above corollary, A is invertible if and only if $rank(A) = n$.

Corollary 8 Let A be an $m \times n$ matrix. Then

- $rank(A^t) = rank(A)$
- $rank(A)$ is equal to the dimension of the row space of A
- dimension of the row space is equal to the dimension of the column space.

Proof. We will show $rank(A^t) = rank(A)$. By the Theorem 3.6, there exits invertible matrices B and C such that $D = BAC$. Then $D^t = (BAC)^t = C^t A^t B^t$. Also, B^t and C^t are invertible. Recall, $(B^t)^{-1} = (B^{-1})^t$. We have $rank(D^t) = r = rank(D)$ and $rank(A) = rank(D) = rank(D^t) = rank(A^t)$. $\square$

Corollary 9 Every invertible matrix is a product of elementary matrices.

Proof. Suppose A is invertible. Then there exists invertible matrices B and C such that $D = BAC$. Thus, D is invertible, which implies $D = I_n$. Also, $B = E_1 \dots E_p$ and $C = G_1 \dots G_q$, where E_i and G_j are elementary. Therefore, $BAC = I_n$ and $A = B^{-1}C^{-1}$. Thus,

$$\begin{aligned} A &= (E_1 \dots E_p)^{-1}(G_1 \dots G_q)^{-1} \\ &= E_p^{-1} \dots E_1^{-1} G_q^{-1} \dots G_1^{-1}. \end{aligned}$$

□

Theorem 3.7. Let $T : V \to W$ and $U : W \to Z$ be linear transformations on finite-dimensional vector spaces. Let A, B be matrices such that AB is defined. Then

(a) $rank(UT) \leq rank(U)$

(b) $rank(UT) \leq rank(T)$

(c) $rank(AB) \leq rank(A)$

(d) $rank(AB) \leq rank(B)$

Proof. (Outline)

- For (a), $R(UT) = U(R(T)) \subseteq U(W) = R(U)$
- (c) and (d) follow from (a) and discussion of the transpose
- (b) follows from the previous by considering matrix representations.

Proof. Let $T : V \to W$ and $U : W \to Z$ be linear transformations on finite-dimensional vector spaces. Let A, B be matrices such that AB is defined. For (a), we have $R(T) = T(V) \subseteq W$. Then

$$\begin{aligned} R(UT) &= (UT)(V) \\ &= U(T(V)) \\ &\subseteq U(W) \\ &= R(U). \end{aligned}$$

Thus, $rank(UT) = dim(R(UT)) \leq dim(R(U)) = rank(U)$.

Now, for (c),

$$\begin{aligned} rank(AB) &= rank(L_{AB}) \\ &= rank(L_A L_B) \\ &\leq rank(L_A) && \text{(By (a))} \\ &= rank(A). \end{aligned}$$

Now, for (d),

$$\begin{aligned} rank(AB) &= rank((AB)^t) \\ &= rank(B^tA^t) \\ &\leq rank(B^t) && \text{(By (c))} \\ &= rank(B). \end{aligned}$$

Now, for (b), let α, β, γ be ordered bases in V, W, and Z. Let $A = \left[U\right]_\beta^\gamma$ and $B = \left[T\right]_\alpha^\beta$. Then $AB = \left[UT\right]_\alpha^\gamma$. Thus,

$$\begin{aligned} rank(UT) &= rank\left(\left[UT\right]_\alpha^\gamma\right) \\ &= rank(AB) \\ &\leq rank(B) && \text{(By (b))} \\ &= rank\left(\left[T\right]_\alpha^\beta\right) \\ &= rank(T). \end{aligned}$$

□

Observations: A is an invertible $n \times n$ matrix if and only if $(A|I_n)$ can be transformed into $(I_n|B)$ by elementary row operations, in this case $B = A^{-1}$.

So, $C = (A|I_n)$. Then $A^{-1}C = (A^{-1}A|A^{-1}) = (I_n|A^{-1})$. Consequently, $A^{-1} = E_1 \dots E_p$ where E_i is elementary. Thus, $(E_1 \dots E_p)C = (I_n|A^{-1})$. So, C can be converted to $(I_n|A^{-1})$ by elementary row operations.

Further, suppose we can transform C to $(I_n|B)$ by using elementary row operations. So, $E_1 \dots E_p(A|I_n) = (I_n|B)$. Let $M = E_1 \dots E_p$. Then, $MA = I_n$ and $M = B$. So, $MA = I_n$ implies $M = A^{-1} = B$. Finally, if A is not invertible, then by Theorem 3.6, $r < n$.

Example: Determine if $\begin{pmatrix} 4 & 0 & 1 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ is invertible and find its inverse.

Solution.

$$\left(\begin{array}{ccc|ccc} 4 & 0 & 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow{\text{Row Op.}} \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 0 & 1 \\ 2 & 1 & 1 & 0 & 1 & 0 \\ 4 & 0 & 1 & 1 & 0 & 0 \end{array}\right)$$

$$\xrightarrow{\text{Row Op.}} \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & -1 & -1 & 0 & 1 & -2 \\ 0 & -4 & -3 & 1 & 0 & -4 \end{array}\right)$$

$$\xrightarrow{\text{Row Op.}} \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & -1 & 2 \\ 0 & 4 & 3 & -1 & 0 & 4 \end{array}\right)$$

$$\vdots$$

$$\xrightarrow{\text{Row Op.}} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & 1 & 0 & -1 & 3 & -2 \\ 0 & 0 & 1 & 1 & -4 & 4 \end{array}\right)$$

Example: Let $T : P_2(\mathbb{R}) \to P_2(\mathbb{R})$ be defined by $T(f) = f + f' + f''$. Find T^{-1}.

Solution. Let $\beta = \{1, x, x^2\}$ be the standard ordered basis for $P_2(\mathbb{R})$. Then

$$\begin{aligned} T(1) &= 1 + 0 + 0 = 1 \\ T(x) &= x + 1 = 1 + x \\ T(x^2) &= x^2 + 2x + 2 = 2 + 2x + x^2. \end{aligned}$$

We have

$$\left[T^{-1}\right]_\beta = \left[T\right]_\beta^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Therefore,

$$\begin{aligned} T^{-1}(a_0 + a_1 x + a_2 x^2) &= \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} \\ &= \begin{pmatrix} a_0 - a_1 \\ a_1 - 2a_2 \\ a_2 \end{pmatrix} \\ &= (a_0 - a_1) + (a_1 - 2a_2)x + a_2 x^2. \end{aligned}$$

3.3 Systems of linear equations (theoretical aspect)

- $Ax = b$ is consistent if it has at least one solution and inconsistent otherwise.

- $Ax = 0$ is called a homogeneous system and $Ax = b$ for $b \neq 0$ a nonhomogeneous system.

Theorem 3.8. Let $Ax = 0$ be a homogeneous system over F in n unknowns and let K be the set of solutions. Then $K = N(L_A)$ and so K is a subspace of $\mathbb{F}^n$ and $dim(K) = n - rank(A)$.

Corollary 12 If $m < n$, then $Ax = 0$ has a non-zero solution.

Proof. We have $dim(K) = dim(N(L_A)) = n - rank(A)$. We know $rank(A) \leq m$. So, $dim(K) = n - rank(A) \geq n - m > 0$. □

Theorem 3.9. Let K be the solution set to $Ax = b$ and K_H be the solution set to $Ax = 0$. Then for any $s \in K$, $K = \{s\} + K_H = \{s + k : k \in K_H\}$.

Proof. Let $s \in K$. Then $K = s + K_H$.

(1) Let $w \in K$. Then $Aw = b$. So, $A(w - s) = Aw - As = b - b = 0$. Thus, $w - s \in K_H$ and we have $w = s + (w - s)$. So, $w \in \{s\} + K_H$.

(2) Let $w \in \{s\} + K_H$. Then $w = s + k$ for some $k \in K_H$, and so $Aw = A(s + k) = As + Ak = b + 0 = b$. Thus, $w \in K$.

□

Theorem 3.10. Let $Ax = b$ be a system of n linear equations in n unknowns. Then A is invertible if and only if the system has exactly one solution. Namely, $x = A^{-1}b$.

Proof. Let $Ax = b$ be a system of n linear equations in n unknowns.

($\Longrightarrow$): Suppose A is invertible. Then $x = A^{-1}b$ is a solution to $Ax = b$. Clearly, $AA^{-1}b = b$. If s is a solution to $Ax = b$, then $As = b$. So, $A^{-1}As = A^{-1}b$ implies $s = A^{-1}b$.

($\Longleftarrow$): Suppose $Ax = b$ has exactly one solution. Let s be this solution. Let K_H be the set of solutions to $Ax = 0$. Then, by theorem 3.9, $\{s\} = \{s\} + K_H$. Thus, $K_H = \{0\}$. Therefore, $N(L_A) = K_H = \{0\}$. Therefore, L_A is injective and surjective. Thus, L_A has an inverse. So, A has an inverse.

□

Theorem 3.11. The system $Ax = b$ is consistent if and only if $rank(A) = rank(A|b)$.

Proof. Note, $R(L_A) = span(\{a_1, \ldots, a_n\})$ where a_i is the ith column of A.

$$\begin{aligned}
Ax = b \text{ is consistent } &\iff b \in R(L_A) \\
&\iff b \in span(\{a_1, \ldots, a_n\}) \\
&\iff span(\{a_1, \ldots, a_n, b\}) = span(\{a_1, \ldots, a_n\}) \\
&\iff dim(span(\{a_1, \ldots, a_n, b\})) = dim(span(\{a_1, \ldots, a_n\})) \\
&\iff rank(A|b) = rank(A).
\end{aligned}$$

□

4 Determinants

4.1 Determinants of order 2

Definition 1 If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then the determinant of A is $ad - bc$.

Notation: The determinant of A will be denoted by $det(A)$ or $|A|$.

Theorem 4.1. For $u, v, w \in \mathbb{F}^2$ and $k \in \mathbb{F}$

$$det\begin{pmatrix} u+kv \\ w \end{pmatrix} = det\begin{pmatrix} u \\ w \end{pmatrix} + k det\begin{pmatrix} v \\ w \end{pmatrix}$$
$$det\begin{pmatrix} w \\ u+kv \end{pmatrix} = det\begin{pmatrix} w \\ u \end{pmatrix} + k det\begin{pmatrix} w \\ v \end{pmatrix}.$$

Theorem 4.2. Let $A \in M_{2\times 2}(\mathbb{F})$. Then the determinant of A is non-zero if and only if A is invertible. If A is invertible, then $A^{-1} = \frac{1}{det(A)}\begin{pmatrix} A_{22} & -A_{12} \\ -A_{21} & A_{22} \end{pmatrix}$.

Proof. Let $A \in M_{2\times 2}(\mathbb{F})$.

($\Longrightarrow$): Let $M = \frac{1}{det(A)}\begin{pmatrix} A_{22} & -A_{12} \\ -A_{21} & A_{11} \end{pmatrix}$. Then,

$$\begin{aligned} AM &= \frac{1}{det(A)}\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}\begin{pmatrix} A_{22} & -A_{12} \\ -A_{21} & A_{11} \end{pmatrix} \\ &= I_2 \\ &= MA. \end{aligned}$$

($\Longleftarrow$): Suppose A is invertible. Then $rank(A) = 2$. If $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$, then $A_{11} \neq 0$ or $A_{12} \neq 0$.

(a) Suppose $A_{11} \neq 0$. Then we can transform A into

$$\begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} - \frac{A_{21}A_{12}}{A_{11}} \end{pmatrix},$$

which has a *rank* of 2. Therefore, $A_{22} - \frac{A_{21}A_{12}}{A_{11}} \neq 0$. Thus, $det(A) \neq 0$.

(b) Suppose $A_{11} = 0$. Then $A_{12} \neq 0$ and $A_{21} \neq 0$. So, $det(A) = -A_{12} - A_{21} \neq 0$.

$\square$

Observation: Let $\delta : M_{2\times 2}(\mathbb{F}) \to \mathbb{F}$ be such that

(1) $\delta \begin{pmatrix} u+kv \\ w \end{pmatrix} = \delta \begin{pmatrix} u \\ w \end{pmatrix} + k\delta \begin{pmatrix} v \\ w \end{pmatrix}$

$\delta \begin{pmatrix} w \\ u+kv \end{pmatrix} = \delta \begin{pmatrix} w \\ u \end{pmatrix} + k\delta \begin{pmatrix} w \\ v \end{pmatrix}$;

(2) $\delta \begin{pmatrix} u \\ u \end{pmatrix} = 0$;

(3) $\delta(I_2) = 1$.

Then $\delta = det$.

Proof. We have

$$\delta\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) + \delta\left(\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\right) = \delta\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)$$
$$\delta\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) + \delta\left(\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\right) = \delta\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right)$$

and

$$\delta\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) + \delta\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right) = \delta\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\right) = 0.$$

Thus,

$$\delta\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) + \delta\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = 0$$

and

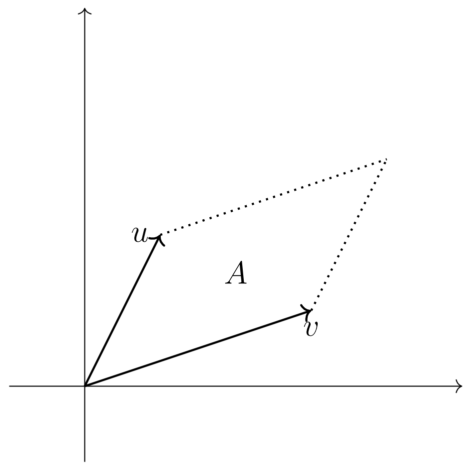
$$\delta\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = -1.$$

Then,

$$\begin{aligned}
\delta\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) &= \delta\left(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}\right) + \delta\left(\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}\right) \\
&= a\delta\left(\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix}\right) + b\delta\left(\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}\right) \\
&= a\left(c\delta\left(\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\right) + d\delta\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\right) + b\left(c\delta\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) + d\delta\left(\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\right)\right) \\
&= ad - bc \\
&= det\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right).
\end{aligned}$$

□

Observation: When $\mathbb{F} = \mathbb{R}$ and $M_{2\times 2}(\mathbb{R})$ and for $\begin{pmatrix} u \\ v \end{pmatrix}$, then we have the following diagram.



We will define the area of the parallelogram to be $A\begin{pmatrix} u \\ v \end{pmatrix}$. If u and v are linearly dependent, then $A\begin{pmatrix} u \\ v \end{pmatrix} = 0$. We can show $A\begin{pmatrix} u \\ v \end{pmatrix} = \operatorname{sign}\left(det\begin{pmatrix} u \\ v \end{pmatrix}\right) det\begin{pmatrix} u \\ v \end{pmatrix}$.

Proof. Define $O : M_{2\times 2}(\mathbb{R}) \to \{-1, 1\}$ by

$$O\begin{pmatrix} u \\ v \end{pmatrix} = \begin{cases} \dfrac{det\begin{pmatrix} u \\ v \end{pmatrix}}{\left|det\begin{pmatrix} u \\ v \end{pmatrix}\right|} & \text{if } u, v \text{ are linearly independent} \\ 1 & \text{if } u, v \text{ are linearly dependent.} \end{cases}$$

Thus, we can show $det\begin{pmatrix} u \\ v \end{pmatrix} = O\begin{pmatrix} u \\ v \end{pmatrix} A\begin{pmatrix} u \\ v \end{pmatrix}$. We will show $\delta\begin{pmatrix} u \\ v \end{pmatrix} = O\begin{pmatrix} u \\ v \end{pmatrix} A\begin{pmatrix} u \\ v \end{pmatrix}$ satisfies the previous observation. Note,

$$\delta\begin{pmatrix} u \\ u \end{pmatrix} = O\begin{pmatrix} u \\ u \end{pmatrix} A\begin{pmatrix} u \\ u \end{pmatrix} = 0 \quad \text{and} \quad \delta\left(I_2\right) = \delta\begin{pmatrix} e_1 \\ e_2 \end{pmatrix} A\begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = 1.$$

We now have three steps.

(a) If $c = 0$, then $\delta\begin{pmatrix} u \\ 0 \end{pmatrix} = 0$. If $c \neq 0$, then $\delta\begin{pmatrix} u \\ cv \end{pmatrix} = O\begin{pmatrix} u \\ cv \end{pmatrix} A\begin{pmatrix} u \\ cv \end{pmatrix}$ and $A\begin{pmatrix} u \\ cv \end{pmatrix} = |c| A\begin{pmatrix} u \\ v \end{pmatrix}$ and $O\begin{pmatrix} u \\ cv \end{pmatrix} = \dfrac{det\begin{pmatrix} u \\ cv \end{pmatrix}}{\left|det\begin{pmatrix} u \\ cv \end{pmatrix}\right|} = \frac{c}{|c|}$. So, $\delta\begin{pmatrix} u \\ cv \end{pmatrix} = c\delta\begin{pmatrix} u \\ v \end{pmatrix}$.

(b) Note, $\delta\begin{pmatrix} u \\ u+v \end{pmatrix} = \delta\begin{pmatrix} u \\ v \end{pmatrix}$. If $a=0$, then $\delta\begin{pmatrix} u \\ au+bv \end{pmatrix} = \delta\begin{pmatrix} u \\ bv \end{pmatrix} = b\delta\begin{pmatrix} u \\ v \end{pmatrix}$. If $a \neq 0$, then

$$\begin{aligned}\delta\begin{pmatrix} u \\ au+bv \end{pmatrix} &= a\delta\begin{pmatrix} u \\ u+\frac{b}{a}v \end{pmatrix} \\ &= a\delta\begin{pmatrix} u \\ \frac{b}{a}v \end{pmatrix} \\ &= b\delta\begin{pmatrix} u \\ v \end{pmatrix}.\end{aligned}$$

(c) Assume $u \neq 0$. Let $w \in \mathbb{R}^2$ such that uw is linearly independent. Then $v_1 = a_1u + b_1w$ and $v_2 = a_2u + b_2w$. So,

$$\begin{aligned}\delta\begin{pmatrix} u \\ v_1+v_2 \end{pmatrix} &= \delta\begin{pmatrix} u \\ (a_1+a_2)u+(b_1+b_2)w \end{pmatrix} \\ &= (b_1+b_2)\begin{pmatrix} u \\ w \end{pmatrix}. && \text{(by (b))}\end{aligned}$$

Also, by (b), $\delta\begin{pmatrix} u \\ v_1 \end{pmatrix} + \delta\begin{pmatrix} u \\ v_2 \end{pmatrix} = b_1\begin{pmatrix} u \\ w \end{pmatrix} + b_2\delta\begin{pmatrix} u \\ w \end{pmatrix}$. Therefore,

$$\delta\begin{pmatrix} u \\ v_1+v_2 \end{pmatrix} = \delta\begin{pmatrix} u \\ v_1 \end{pmatrix} + \delta\begin{pmatrix} u \\ v_2 \end{pmatrix}.$$

□

4.2 Determinants of order n

Let $\tilde{A}_{ij}$ be the matrix obtained from A by deleting the ith row and the jth column.

Definition 2 Let $A \in M_{n\times n}(\mathbb{F})$.

- If $n = 1$, then $det(A) = A_{11}$.
- If $n \geq 2$, then $det(A) = \sum_{j=1}^{n}(-1)^{1+j}A_{1j}det(\tilde{A}_{1j})$.

The cofactor of the i,jth entry of A,

$$c_{ij} = (-1)^{i+j}det(\tilde{A}_{ij}).$$

Example:

$$\begin{vmatrix} 0 & 1 & 3 \\ -2 & -3 & -5 \\ 4 & -4 & 4 \end{vmatrix} = 0 \cdot (-1)^2 \cdot \begin{vmatrix} -3 & -5 \\ -4 & 4 \end{vmatrix} + 1 \cdot (-1)^3 \cdot \begin{vmatrix} -2 & -5 \\ 4 & 4 \end{vmatrix} + 3 \cdot (-1)^4 \cdot \begin{vmatrix} -2 & -3 \\ 4 & -4 \end{vmatrix}$$
$$= 0 - 12 + 60$$
$$= 48.$$

Theorem 4.3. Let $a_1, \ldots, a_n \in \mathbb{F}^n$, let $k \in \mathbb{F}$ and suppose $a_r = u + kv$ for some $u, v \in \mathbb{F}^n$. Then

$$\begin{vmatrix} a_1 \\ a_{r-1} \\ a_r \\ a_{r+1} \\ a_n \end{vmatrix} = \begin{vmatrix} a_1 \\ a_{r-1} \\ u \\ a_{r+1} \\ a_n \end{vmatrix} + k \begin{vmatrix} a_1 \\ a_{r-1} \\ v \\ a_{r+1} \\ a_n \end{vmatrix}.$$

Corollary 4 If A has a row consisting of zeroes, then $det(A) = 0$.

Lemma 5. Let $B \in M_{n\times n}(\mathbb{F})$ and $n \geq 2$. Suppose that the ith row of B is e_k for some $1 \leq k \leq n$. Then $det(B) = (-1)^{i+k} det(\tilde{B}_{ik})$.

Theorem 4.4. For $A \in M_{n\times n}(\mathbb{F})$ and $i \in \{1, \ldots, n\}$

$$det(A) = \sum_{j=1}^{n} (-1)^{i+j} A_{ij} det(\tilde{A}_{ij}).$$

Corollary 7 If $A \in M_{n\times n}(\mathbb{F})$ has two identical rows, then $det(A) = 0$.

Proof. Let $a_r = u + kv$.

(Base Case): Let $n = 1$. Then clearly, $det(A) = 0$.

(Inductive Step): Let $n \geq 2$. If $r = 1$, then $A_{1j} = u_j + kv_j$. Let B and C be matrices obtained from A by replacing row r by u and v. Then

$$det(\tilde{A}_{1j}) = det(\tilde{B}_{1j}) = det(\tilde{C}_{1j}).$$

Thus,

$$\begin{aligned} det(A) &= \sum_{j=1}^{n} (-1)^{1+j} A_{1j} det(\tilde{A}_{1j}) \\ &= \sum_{j=1}^{n} (-1)^{1+j} B_{1j} det(\tilde{B}_{1j}) + \sum_{j=1}^{n} (-1)^{1+j} C_{1j} det(\tilde{C}_{1j}) \\ &= det(B) + k det(C). \end{aligned}$$

□

Theorem 4.5. If $A \in M_{n\times n}(\mathbb{F})$ and B is obtained from A by interchanging two rows, then $det(B) = -det(A)$.

Proof. Say rows a_r and a_s are interchanged. Play with the matrix that has rows r and s equal to $a_r + a_s$. □

Theorem 4.6. If $A \in M_{n\times n}(\mathbb{F})$ and B is obtained from A by adding a multiple of one row to another, then $det(B) = det(A)$.

Proof. Use expansion formula from Theorem 4.4. □

Corollary 10 If $A \in M_{n\times n}(\mathbb{F})$ and $rank(A) < n$, then $det(A) = 0$.

Proof. Rows of A are linearly dependent so say $a_1 = \sum_{i\geq 2} c_i a_i$. Use Theorem 4.6. □

4.3 Properties

Summary of properties

- Let $A, B \in M_{n\times n}(\mathbb{F})$. Then $det(AB) = det(A)det(B)$.
- $A \in M_{n\times n}(\mathbb{F})$ is invertible if and only if $det(A) \neq 0$ and $det(A^{-1}) = \frac{1}{det(A)}$.
- Let $A \in M_{n\times n}(\mathbb{F})$. Then $det(A^t) = det(A)$.
- (Cramer's Rule) Let $Ax = b$ where $A \in M_{n\times n}(\mathbb{F})$ and let M_k be the $n \times n$ matrix obtained from A by replacing column k with b. Then $x_k = \frac{det(M_k)}{det(A)}$.

5 Diagonalization

5.1 Eigenvalues and eigenvectors

Definition 1 Let V be finite-dimensional and let $T : V \to V$ be linear. T is called *diagonalizable* if there is an ordered basis β such that $[T]_\beta$ is a diagonal matrix.

Matrix A is diagonalizable if L_A is.

Definition 2 A non-zero vector $v \in V$ such that $T(v) = \lambda v$ for some $\lambda \in \mathbb{F}$ is called an *eigenvector*. The scalar λ is called an *eigenvalue* of T.

Theorem 5.1. Let V be finite-dimensional. A linear operator on V is diagonalizable if and only if there is an ordered basis β for V consisting of eigenvectors.

Theorem 5.2. Let $A \in M_{n\times n}(\mathbb{F})$. Then $\lambda \in \mathbb{F}$ is an eigenvalue of A if and only if $det(A - \lambda I_n) = 0$.

Definition 3

- Let $A \in M_{n\times n}(\mathbb{F})$. Then $f(t) = det(A - \lambda I_n)$ is called the *characteristic polynomial* of A.
- If T is a linear operator V, then the characteristic polynomial of T is the characteristic polynomial of $A = \big[T\big]_\beta$ where β is an ordered basis for V.

Note: The characteristic polynomial of T is well-defined.

Theorem 5.3. Let $A \in M_{n\times n}(\mathbb{F})$.

- $f_A(t)$ is a polynomial of degree n with the leading coefficient $(-1)^n$.
- A has at most n distinct eigenvalues.

Theorem 5.4. Let T be a linear operator on V and let λ be an eigenvalue of T. A vector $v \in V$ is an eigenvector of T corresponding to λ if and only if $v \neq 0$ and $v \in N(T - \lambda I)$.

5.2 Diagonalizability

Theorem 5.5. Let T be a linear operator with distinct eigenvalues $\lambda_1, \dots, \lambda_k$. If $v_1, \dots, v_k$ are eigenvectors of T such that v_i corresponds to λ_i, then $\{v_1, \dots, v_k\}$ is linearly independent.

Corollary 6 If T has n distinct eigenvalues, then T is diagonalizable.

Definition 4 A polynomial $f(t) \in P(\mathbb{F})$ splits over $\mathbb{F}$ if $f(t) = c(t-a_1)\dots(t-a_n)$ for some $c, a_1, \dots, a_n \in \mathbb{F}$.

Theorem 5.6. Let T be a linear operator. If T is diagonalizable, then its characteristic polynomial splits.

Definition 5 The (algebraic) *multiplicity* of an eigenvalue λ is the largest positive integer k such that $(t-\lambda)^k | f(t)$.

The eigenspace of T with respect to λ is

$$E_\lambda = N(T - \lambda I_V) = \{x \in V | T(x) = \lambda x\}.$$

Theorem 5.7. Let λ be an eigenvalue of T of multiplicity m. Then

$$1 \leq dim(E_\lambda) \leq m.$$

Proof. (Outline)

- Start with an ordered basis $\{v_1, \ldots, v_p\}$ for E_λ and extend it to an ordered basis β for V.
- Then $A = \big[T\big]_\beta$ will have the following form

$$\begin{pmatrix} \lambda I_p & B \\ 0 & C \end{pmatrix}.$$

Lemma 9. Let $\lambda_1, \ldots, \lambda_k$ be distinct eigenvalues of T and let $v_i \in E_{\lambda_i}$. If $v_1 + \cdots + v_k = 0$, then $v_i = 0$ for every i.

Theorem 5.8. Let $\lambda_1, \ldots, \lambda_k$ be distinct eigenvalues of T and let $S_i \subseteq E_{\lambda_i}$ be finite and linearly independent. Then $S_1 \cup \cdots \cup S_k$ is linearly independent.

Proof. (Outline) Say $S_i = \{v_{i_1}, \ldots, v_{i_{n_i}}\}$ and suppose $\sum_{i=1}^{k} \sum_{j=1}^{n_i} a_{ij} v_{i_j} = 0$. Consider $w_i = \sum_{j=1}^{n_i} a_{ij} v_{i_j}$.

Theorem 5.9. Let T be a linear operator on a finite-dimensional vector space V such that the characteristic polynomial of T splits. Let $\lambda_1, \ldots, \lambda_k$ be distinct eigenvalues of T. Then

(a) T is diagonalizable if and only if the multiplicity of each λ_i equals $dim(E_{\lambda_i})$.

(b) If T is diagonalizable and β_i is an ordered basis for E_{λ_i}, then $\beta = \beta_1 \cup \cdots \cup \beta_k$ is an ordered basis for V.

Proof. (Outline)

- Part (b) follows from the proof.
- ($\Longrightarrow$): m_i- the multiplicity of λ_i, $d_i = dim(E_{\lambda_i})$, $\beta_i = \beta \cap E_{\lambda_i}$, $n_i = |\beta_i|$. We have $n_i \leq d_i \leq m_i$ and $\sum n_i = n = \sum m_i$. It follows that $d_i = m_i$ for every i.
- ($\Longleftarrow$): Let β_i be an ordered basis for E_{λ_i}; let $\beta = \beta_1 \cup \cdots \cup \beta_k$. Then β is a basis for V consisting of eigenvectors.

Note: T is diagonalizable if and only if

- The characteristic polynomial splits and
- the multiplicity of λ_i is $nullity(T - \lambda_i I) = n - rank(T - \lambda_i I)$.

5.4 Invariant subspaces and the Cayley-Hamilton theorem

Definition 6

- Let $T : V \to V$. A subspace $W \subseteq V$ is called a T-invariant subspace of V if $T(W) \subseteq W$.
- The T-cycle subspace of V generated by x is

$$span(\{x, T(x), T^2(x), \dots\}).$$

Note: T-cyclic subspace is a minimal subspaces which is T-invariant and contains x.

Theorem 5.21. Let T be a linear operator on a finite-dimensional vector space V and let W be a T-invariant subspace of V. Then the characteristic polynomial of the restriction of T to W, T_W, divides the characteristic polynomial of T.

Theorem 5.22. Let T be a linear operator on a vector space V of dimension n and let W be a T-cyclic subspace of V generated by a non-zero vector v of dimension k. Then

(a) $\{v, T(v), \dots, T^{k-1}(v)\}$ is a basis for W.

(b) If $a_0 + a_1T(v) + \cdots + a_{k-1}T^{k-1}(v) + T^k(v) = 0$, then the characteristic polynomial of T_W is $f(t) = (-1)^k(a_0 + a_1t + \cdots + a_{k-1}t^{k-1} + t^k)$.

Proof. (Outline)

(a) Let j be the largest integer such that $\beta = \{v, T(v), \dots, T^{j-1}(v)\}$ is linearly independent. Then $span(\beta)$ is T-invariant and it follows that $j = k$.

(b) Let $\beta = v, T(v), \dots, T^{k-1}(v)$ and suppose $a_0v + a_1T(v) + \cdots + a_{k-1}T^{k-1} + T^k(v) = 0$. Use the form of $\left[T_W\right]_\beta$ to notice that $f_{T_W}(t) = (-1)^k(a_0 + a_1t + \cdots + a_{k-1}t^{k-1} + t^k)$.

Theorem 5.23, Cayley-Hamilton. Let V be finite-dimensional and let $T : V \to V$ be linear with the characteristic polynomial $f(t)$. Then $f(T) = T_0$.

Proof. Note that $f(T)$ is a linear operator. We will show $f(T)(v) = 0$ for every v.

- Take $v \neq 0$ and consider the T-cycle subspace generated by v, W.
- Let $k = dim(W)$. Then $T^k \in span(\{v, T(v), \dots, T^{k-1}(v)\})$ by 5.22(a) and we are done by 5.22(b).

□

Corollary 15 Let A be an $n \times n$ matrix and let $f(t)$ be its characteristic polynomial. Then $f(A) = 0_n$, the $n \times n$ zero matrix.

6 Inner product spaces

6.1 Inner products and norms

Definition 1 Let V be a vector space over F . An *inner product* on V is a function $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$ such that the following conditions hold.

- $\langle x+z, y \rangle = \langle x, y \rangle + \langle z, y \rangle$
- $\langle cx, y \rangle = c\langle x, y \rangle$
- $\overline{\langle x, y \rangle} = \langle x, y \rangle$
- $\langle x, x \rangle > 0$ if $x \neq 0$ and $\langle 0, 0 \rangle = 0$.

Definition 2 The *adjoint* of an $m \times n$ matrix X is the $n \times m$ matrix A^* such that $(A^*)_{ij} = \overline{A_{ji}}$.

Theorem 6.1.

- $\langle x, y+z \rangle = \langle x, y \rangle + \langle x, z \rangle$
- $\langle x, cy \rangle = \bar{c}\langle x, y \rangle$
- $\langle x, 0 \rangle = \langle 0, x \rangle = 0$
- $\langle x, x \rangle = 0$ if and only if $x = 0$
- If $\langle x, y \rangle = \langle x, z \rangle$ for every $x \in V$, then $y = z$.

Definition 3 Let V be an inner product space. For $x \in V$, the *norm* of x is $\|x\| = \sqrt{\langle x, x \rangle}$.

Theorem 6.2. Let V be an inner product space over F. For $x, y \in V$ and $c \in \mathbb{F}$.

(a) $\|cx\| = |c| \cdot \|x\|$

(b) $\|x\| = 0$ if and only if $x = 0$ and $\|x\| \geq 0$ for any x.

(c) (Cauchy-Schwarz Inequality) $|\langle x, y \rangle| \leq \|c\|\|y\|$

(d) (Triangle Inequality) $\|x+y\| \leq \|x\| + \|y\|$

Proof. (Outline)

(c) Expand $\|x - cy\|^2$ and apply with $c = \frac{\langle x,y \rangle}{\langle y,y \rangle}$

(d) Note that $\langle x, y \rangle + \langle y, x \rangle = 2Re\langle x, y \rangle$ and $Re\langle x, y \rangle \leq |\langle x, y \rangle|$.

Definition 4

- Vectors $x, y \in V$ are called *orthogonal* if $\langle x, y\rangle = 0$.
- A set of vectors $S \subseteq V$ is called *orthogonal* if any two distinct vectors are orthogonal.
- S is called *orthonormal* if it is orthogonal and $\|x\| = 1$ for every $x \in S$.

Old Town Problem: There are n people living in an odd town and they form clubs. A club must contain an odd number of members and for any two distinct clubs there must be an even (possibly zero) number of people in both of them. What is the maximum number of clubs that can be formed?

6.2 The Gram-Schmidt orthogonalization

Definition 5 An ordered basis which is orthonormal is called an *orthonormal basis.*

Theorem 6.3. Suppose $S = \{v_1, \ldots, v_k\}$ is an orthogonal subset of V such that $v_i \neq 0$. For $y \in span(S)$,

$$y = \sum_{i=1}^{k} \frac{\langle y, v_i\rangle}{\|v_i\|^2} v_i.$$

Corollary 4 Any orthogonal set of non-zero vectors is linearly independent.

Theorem 6.4 (Graham-Schmidt algorithm). Let $S = \{w_1, \ldots, w_n\}$ be a linearly independent subset. Define $S' = \{v_1, \ldots, v_n\}$ as follows, $v_1 := w_1$ and for $k \geq 2$

$$v_k = w_k - \sum_{j=1}^{k-1} \frac{\langle w_k, v_j\rangle}{\|v_j\|^2} v_j.$$

Then S' is orthogonal and $span(S') = span(S)$.

Proof. This is induction on $|S|$. For the inductive step, first check that $v_k \neq 0$ and then compute $\langle v_k, v_i\rangle$ for $i < k$. Then $dim(span(S'_k)) = dim(span(S_k))$ because S'_k is linearly independent. □

Theorem 6.5. Let V be a finite-dimensional inner product space and let $\beta = \{v_1, \ldots, v_n\}$ be an orthonormal basis for V. Then for every $x \in V$, $x = \sum_{i=1}^{n} \langle x, v_i\rangle v_i$.

Corollary 7 Let $\beta = \{v_1, \ldots, v_n\}$ be orthonormal, let $T : V \to V$ be linear, and let $A = \left[T\right]_\beta$. Then $A_{ij} = \langle T(v_j), v_i\rangle$.

Fourier coefficient of x relative to β is $\langle x, y\rangle$ where $y \in \beta$.

Definition 6 Let S be a non-empty subset of V. Define $S^{\perp} = \{x \in V : \langle x, y\rangle = 0 \text{ for every } y \in S\}$.

Note: $S^{\perp}$ is a subspace of V.

Theorem 6.6. Let W be a finite-dimensional subspace of an inner product space V and let $y \in V$. Then the exist unique $u \in W$ and $z \in W^{\perp}$ such that $y = u + z$. Furthermore, if $\{v_1, \ldots, v_k\}$ is an orthonormal basis for W, then $u = \sum\langle y, v_i\rangle v_i$.

Proof. (Outline)

- Let $u = \sum\langle y, v_i\rangle v_i$ and $z = y - u$. Check that $z \in W^{\perp}$.
- For the uniqueness $u - u' \in W$ and $z' - z \in W^{\perp}$.

Corollary 9 For any $x \in W$, $\|y - x\| \geq \|y - u\|$ and if $\|y - x\| = \|y - u\|$ then $x = u$.

Theorem 6.7. Suppose $S = \{v_1, \ldots, v_k\}$ is an orthonormal set in an n-dimensional inner product space V. Then

(a) S can be extended to an orthonormal basis $\{v_1, \ldots, v_n\}$ for V.

(b) $\{v_{k+1}, \ldots, v_n\}$ is an orthonormal basis for $(span(S))^{\perp}$.

(c) If W is a subspace of V, then $dim(W) + dim(W^{\perp}) = dim(V)$.

6.3 The adjoint of a linear operator

Theorem 6.8. Let V be a finite-dimensional inner product space over F, and let $g : V \to \mathbb{F}$ be a linear transformation. Then there exists a unique vector $y \in V$ such that $g(x) = \langle x, y\rangle$ for every $x \in V$.

Proof. (Outline) Take an orthonormal basis $\beta = \{v_1, \ldots, v_n\}$ and define $y = \sum \overline{g(v_i)} v_i$.

Theorem 6.9. Let V be a finite-dimensional inner product space and let $T : V \to V$ be linear. Then there exists a unique function $T^* : V \to V$ such that $\langle T(x), y\rangle = \langle x, T^*(y)\rangle$ for all x, y. Furthermore, T^* is linear.

Proof. (Outline)

- Fix y. Check that $g(x) = \langle T(x), y\rangle$ is linear.
- Theorem 6.8 gives unique y' such that $g(x) = \langle x, y'\rangle$. Define $T^*(y) = y'$.
- Note that T^* is a function and check that it is linear.

Theorem 6.10. Let V be a finite-dimensional inner product space and let β be an orthonormal ordered basis for V. If T is a linear operator on V, then $\left[T^*\right]_\beta = \left[T\right]_\beta^*$.

Theorem 6.11. Let V be an inner-product space, and let T, U be linear operators on V. Then

(a) $(T+U)^* = T^* + U^*$

(b) $(cT)^* = \overline{c}T^*$

(c) $(TU)^* = U^*T^*$

(d) $T^{**} = T$

(e) $I^* = I$

6.4 Normal and self-adjoint operators

Lemma 15. Let T be a linear operator on a finite-dimensional inner product space V. If T has an eigenvector, then so does T^*.

Theorem 6.14 (Schur). Let T be a linear operator on a finite-dimensional inner product space V and suppose that the characteristic polynomial of T splits. Then there exists an orthonormal basis β for V such that $\left[T\right]_\beta$ is upper triangular.

Proof. (Outline)

- Show that $W^\perp$ is T-invariant and $dim(W^\perp) = n-1$.
- The characteristic polynomial of $T_{W^\perp}$ divided $f_T(t)$ (so it splits) and by **IH** for some γ, $\left[T_{W^\perp}\right]_\gamma$ is upper-triangular.
- Let $\beta = \gamma \cup \{z\}$ Then $\left[T\right]_\beta$ is upper-triangular.

Note: If V has an orthonormal basis of eigenvectors of T, then $TT^* = T^*T$.

Definition 7 $T : V \to V$ is *normal* if $TT^* = T^*T$. $A \in M_{n\times n}(\mathbb{F})$ is *normal* if $AA^* = A^*A$.

Theorem 6.15. Let T be a normal operator on V. Then

(a) $\|T(x)\| = \|T^*(x)\|$

(b) $T - cI$ is normal for every $c \in \mathbb{F}$.

(c) If x is an eigenvector of T, then x is an eigenvector of T^*.

(d) If λ_1, λ_2 are distinct eigenvalues of T with eigenvectors x_1, x_2, then $\langle x_1, x_2 \rangle = 0$.

Theorem 6.16. Let T be a linear operator on a finite-dimensional complex inner-product space V. Then T is normal if and only if there exists an orthonormal basis for V consisting of eigenvectors of T.

Proof. (Outline) Suppose T is normal.

- T splits over C and so apply Schur's lemma to get an orthonormal basis $\beta = \{v_1, \ldots, v_n\}$.
- $A := [T]_\beta$ is upper-triangular and so $T(v_1) = A_{11}v_1$.
- Show that e_k is an eigenvector by induction on k using the fact that $A_{jk} = \langle T(v_k), v_j \rangle$.

The converse is easy.

Definition 8 $T : V \to V$ is *self-adjoint* (Hermitian) if $T = T^*$. $A \in M_{n\times n}(\mathbb{F})$ is *Hermitian* if $A = A^*$.

Lemma 19. Let T be a Hermitian operator on a finite-dimensional inner product space V. Then,

(a) All eigenvalues of T are real.

(b) If V is a real inner product space, then the characteristic polynomial splits.

Theorem 6.17. Let T be a linear operator on a finite-dimensional real inner-product space V. Then T is Hermitian if and only if there exists an orthonormal basis for V consisting of eigenvectors of T.

Proof. The characteristic polynomial splits and so we may apply Schur's lemma. $A := [T]_\beta$ is upper-triangular and so A^*. Thus it must be a diagonal matrix. □

6.5 Unitary and orthogonal operators and their matrices

Definition 9 Let V be a finite-dimensional inner-product space over F and let $T : V \to V$ be linear. If $\|T(x)\| = \|x\|$ for every $x \in V$, then T is called *unitary* if $\mathbb{F} = \mathbb{C}$ and orthogonal if $\mathbb{F} = \mathbb{R}$.

Theorem 6.18. Let T be a linear operator on a finite-dimensional inner-product space V. Then the following statements are equivalent.

(a) $TT^* = T^*T = I$

(b) $\langle T(x), T(y)\rangle = \langle x, y\rangle$ for all $x, y \in V$

(c) If β is an orthonormal basis, then so is $T(\beta)$.

(d) There exists an orthonormal basis β such that $T(\beta)$ is orthonormal.

(e) $\|T(x)\| = \|x\|$ for every x.

Proof. (Outline)

- *(d)* $\Longrightarrow$ *(e)* Let $\beta = \{v_1, \ldots, v_n\}$ be orthonormal such that $T(\beta)$ is orthonormal. Take $x \in V$. Then $x = \sum a_i v_i$ and
$$\|x\|^2 = \sum |a_i|^2 = \sum \|T(x)\|^2.$$
- *(e)* $\Longrightarrow$ *(a)* $\langle x, x\rangle = \langle x, T^*T(x)\rangle$ be (e). Thus $\langle x, (I - T^*T)(x)\rangle = 0$ for every x. Set $U := I - T^*T$. Then U is self-adjoint and so there is an orthonormal basis consisting of eigenvectors of U. Check that $U(x) = \lambda x$ implies $\lambda = 0$; $U = T_0$; $T^*T = I$; $TT^* = I$ as well because $\big[T\big]_\beta$ is a square matrix.

Definition 10 A square matrix A is called *orthogonal* if $A^tA = AA^t = I$ and *unitary* if $A^*A = AA^* = I$.

Note:

- $AA^* = I$ if and only if A are orthonormal.
- $A^*A = I$ if and only if columns of A are orthonormal.
- If λ is an eigenvalue of a unitary (orthogonal) matrix, then $|\lambda| = 1$.

Definition 11 $A, B \in M_{n\times n}(\mathbb{C})$ $(A, B \in M_{n\times n}(\mathbb{R}))$ are *unitarily (orthogonally) equivalent* if there exists a unitary (orthogonal) matrix P such that $A = P^{-1}BP$.

Theorem 6.19. Let $A \in M_{n\times n}(\mathbb{C})$. Then A is normal if and only if A is unitarily equivalent to a diagonal matrix.

Theorem 6.20. Let $A \in M_{n\times n}(\mathbb{R})$. Then A is symmetric if and only if A is orthogonally equivalent to a diagonal matrix.

Theorem 6.21 (Schur). Let $A \in M_{n\times n}(\mathbb{F})$ and suppose $f_A(t)$ splits over $\mathbb{F}$.

(a) If $\mathbb{F} = \mathbb{C}$, then A is unitarily equivalent to a complex upper-triangular matrix.

(b) If $\mathbb{F} = \mathbb{R}$, then A is orthogonally equivalent to a real upper-triangular matrix.