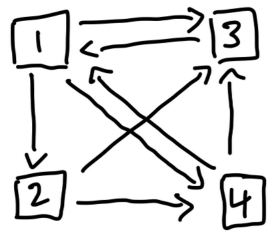
MATH 4310 Lecture Notes (Dylan Tom)

Introduction & Fields



Question: How do we determine the page order for a mini "google"?

1. (Simple Approach) Determine the importance by the number of back links (we expect page 3 should be the top*)
2. (Weighted Approach) Back links from "important" pages should weigh more. Let the "score" of a page be the sum of the scores of its back links.
3. Prevent undue influence by one page linking to too many other pages. If page j contains n_j links, one of which is page k, then boost the score of page k by $\frac{x_j}{n_j}$ where x_j is the score of page j

In our example,

$$\begin{aligned} x_1 &= \frac{1}{1}x_3 + \frac{1}{2}x_4 \\ x_2 &= \frac{1}{3}x_1 \\ x_3 &= \frac{1}{3}x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_4 \\ x_4 &= \frac{1}{3}x_1 + \frac{1}{2}x_2 \end{aligned}$$

Answer: $x_1 = \frac{12}{31} \quad x_2 = \frac{4}{31} \quad x_3 = \frac{9}{31} \quad x_4 = \frac{6}{31}$

*We have shown that page 1 should be ranked higher than 3, so our intuition wasn't correct.

Question: What are some properties of the set of real numbers with addition and multiplication?

1. There is a $0 \in S$ such that $0 + a = a$ for all $a \in S$
2. There is a $1 \in S$ such that $1 \cdot a = a$ for all $a \in S$
3. commutativity, associativity, distributivity
4. There exists a $(-a) \in S$ such that $a + (-a) = 0$ for all $a \in S$

5. There exists a $a^{-1} \in S$ such that $aa^{-1} = 1$ for all $a \in S$
6. $a - b = a + (-b)$ and $\frac{a}{b} = a \cdot b^{-1}$

Question: What sets have these properties?

$$\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p$$

Question: What sets do not satisfy these properties?

$$\mathbb{Z}, \mathbb{N}, \mathbb{M}_{2\times 2}$$

Definition. A **field**, $\mathbb{F}$, is a set on which addition $(+)$ and multiplication $(\cdot)$ are defined so that the following properties hold for all $a, b, c \in \mathbb{F}$.

1. $a + b = b + a \quad a \cdot b = b \cdot a$ (commutativity)
2. $(a + b) + c = a + (b + c) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativity)
3. There exists *distinct* elements $0, 1$ such that $0 + a = a$ and $1 \cdot a = a$ (identity)
4. There exists $c, d \in \mathbb{F}$ such that $a + c = 0$ and $bd = 1$ where $d \neq 0$ (invertibility). Define $c = -a$ and $d = b^{-1}$ (see uniqueness below)
5. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (distributivity)

Example: Some fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F} = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}, \mathbb{F}_2 = \{0, 1\}$

Example: Cancellation Laws

1. $a + b = a + c \Rightarrow b = c$

   Proof. Let's assume $a + b = a + c$. By (4), there is some x such that $x + a = 0$. Now $x + (a + b) = x + (a + c)$. By (2), $(x + a) + b = (x + a) + c \Rightarrow 0 + b = 0 + c$. By (3), $b = c$. □

2. $a \cdot b = a \cdot c$ and $a \neq 0 \Rightarrow b = c$

   Proof. Let's assume $a \cdot b = a \cdot c$ and $a \neq 0$. By (4), there is some x such that $ax = 1$. Now $x(ab) = x(ac)$. By (2), $(xa)b = (xa)c \Rightarrow 1b = 1c$. By (3), $b = c$. □

Example: Uniqueness of 0, 1, additive inverse, and multiplicative inverse

Proof. (multiplicative inverse) Given $b \neq 0$, let d and d' satisfy $b \cdot d = 1$ and $b \cdot d' = 1$. Then, $b \cdot d = b \cdot d'$. So, $d = d'$ (by cancellation). Similarly, for others. □

Example: Some more properties of fields

1. $a \cdot 0 = 0$

   Proof. $(a \cdot 0) + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \Rightarrow 0 = a \cdot 0$ □

2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

   Proof. $[(-a) \cdot b] + [a \cdot b] = b \cdot (a + (-a)) = b \cdot 0 = 0$
   $[a \cdot (-b)] + [a \cdot b] = a \cdot (b + (-b)) = a \cdot 0 = 0$ □

3. $(-a) \cdot (-b) = a \cdot b$

   Proof. $(-a) \cdot (-b) = -[a \cdot (-b)] = -[-(a \cdot b)] = a \cdot b$ □

Properties of Relations:

1. Reflexive: $\forall a \in S$, $a \sim a$
2. Symmetric: $\forall a, b \in S$, if $a \sim b$, then $b \sim a$
3. Transitive: $\forall a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$

An equivalence relation satisfies all 3 of these properties

Example: Define $S = \{\text{all humans}\}$. $a \sim b$ if a and b share a parent. It is reflexive, symmetric, but not transitive.

Definition. The class of a is all elements related to a, denoted by $[a]$. There can be no intersection between two classes.

Example: Define $S = \mathbb{Z}$. $a \sim b$ if $a - b$ is even. This is an equivalence relation. We can partition $\mathbb{Z}$ into even and odd, $[0]$ and $[1]$. We call this $\mathbb{Z}_2 = \mathbb{F}_2$.

In general, fix $d \geq 1$. Define $a \sim b$ if $a - b$ is divisible by d. In $\mathbb{Z}_d$,

1. $[a] + [b] = [(a + b) \mod d]$
2. $[a] \cdot [b] = [(a \cdot b) \mod d]$

Question: When is $\mathbb{Z}_d$ a field? Only if d is prime.

Vector Spaces

Definition. Let $\mathbb{F}$ be a field. A vector (linear) space, V over $\mathbb{F}$ is a set with two operations, addition $(+) : V \times V \to V$ and scalar multiplication $(\cdot) : \mathbb{F} \times V \to V$. For all vectors, $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$ and $a, b \in \mathbb{F}$.

- $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$
- $\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}$
- There is a 0 such that $0 + \mathbf{x} = \mathbf{x}$
- There is a $\mathbf{y}$ such that $\mathbf{x} + \mathbf{y} = 0$
- There is a 1 such that $1 \cdot \mathbf{x} = \mathbf{x}$
- $(ab)\mathbf{x} = a(b\mathbf{x})$
- $a \cdot (\mathbf{x} + \mathbf{y}) = (a \cdot \mathbf{x}) + (a \cdot \mathbf{y})$
- $(a + b)\mathbf{x} + a\mathbf{x} + b\mathbf{x}$

Question: Are the following vector spaces?

1. $D(\mathbb{R}, \mathbb{R})$, the set of all differentiable functions, $f : \mathbb{R} \to \mathbb{R}$
   Yes, we can show that this set is closed under addition and scalar multiplication.

2. S, the set of all polynomials of degree n with coefficients over the field, $\mathbb{F}$
   No, take $p(x) = x^n$ and $q(x) = -x^n$ so $p(x) + q(x) = 0$, which is not a polynomial of degree n. It is not closed under addition. **Be careful**, polynomials of degree less than or equal to n form a vector space.

Claim: The zero vector is unique.

Proof. Assume that $\mathbf{0}_1$ and $\mathbf{0}_2$ are two zero vectors. Then, $\mathbf{0}_1 = \mathbf{0}_1 + \mathbf{0}_2 = \mathbf{0}_2$. □

Claim: Given $\mathbf{x} \in V$, there exists a unique $\mathbf{y} \in V$ such that $\mathbf{x} + \mathbf{y} = \mathbf{0}$

Proof. Let $\mathbf{y}_1$ and $\mathbf{y}_2$ be two such vectors. Then, $\mathbf{y}_1 = \mathbf{y}_1 + \mathbf{0} = \mathbf{y}_1 + (\mathbf{x} + \mathbf{y}_2) = (\mathbf{y}_1 + \mathbf{x}) + \mathbf{y}_2 = \mathbf{0} + \mathbf{y}_2 = \mathbf{y}_2$. □

Bold face for vectors will be dropped unless it needs to be distinguished.

Claim: Let $u, v, w \in V$, if $u + v = u + w$, then $v = w$.

$$\begin{aligned} u + v &= u + w \\ (-u) + (u + v) &= (-u) + (u + w) \\ (-u + u) + v &= (-u + u) + w \\ 0 + v &= 0 + w \\ v &= w \end{aligned}$$

Claim: $a \cdot \mathbf{0} = \mathbf{0}$

$$\begin{aligned} &a \cdot \mathbf{0} = a \cdot (\mathbf{0} + \mathbf{0}) = a \cdot \mathbf{0} + a \cdot \mathbf{0} \\ &a \cdot \mathbf{0} = a \cdot \mathbf{0} + \mathbf{0} \end{aligned}$$

By cancellation, $a \cdot \mathbf{0} = \mathbf{0}$

Claim: $0 \cdot a = \mathbf{0}$

$$0 \cdot a + 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a = 0 \cdot a + 0$$

By cancellation, $0 \cdot a = \mathbf{0}$.

Claim: Define $-x = (-1) \cdot x$. Show that this is the additive inverse of x.

Proof. $(-1)x + x = (-1)x + 1x = (-1 + 1)x = 0x = \mathbf{0}$ □

Example: Vector Spaces

- $\mathbb{F}^n$ is the space of n-tuples
- $\mathbb{M}_{2\times3}(\mathbb{F})$ space of 2×3 matrices
- $\mathcal{F}(S, \mathbb{F}) = \{f : S \to \mathbb{F}\}$
- $\mathcal{P}(\mathbb{F})$ is space of all polynomials

Aside: As a vector space over $\mathbb{F}$, $\mathbb{F}^n$ is equivalent to $\mathbb{M}_{2\times3}(\mathbb{F})$

Example: Non Vector Spaces

- $\{(x, y) \in \mathbb{R}^2 | x, y \geq 0\}$
- $\mathbb{R}^2$; $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 - b_2)$
- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}\}$

Definition. Let V be a vector space over $\mathbb{F}$. A subset $W \subset V$ is called a subspace if

1. $0 \in W$
2. If $x, y \in W$, then $x + y \in W$
3. If $x \in W$, then $cx \in W$ for all $c \in \mathbb{F}$

Example: Subspaces

- $V = \mathbb{F}^{n\times 1}$; $W = \{x \in \mathbb{F}^{n\times 1} : Ax = 0\}$

  Proof. $0_{n\times 1} \in W$ because $A0 = 0$. W is closed under addition because $x, y \in W$,

  $$Ax = 0, Ay = 0 \implies A(x + y) = Ax + Ay = 0 + 0 = 0$$

  W is closed under scalar multiplication because $x \in W$, $c \in \mathbb{F}$,

  $$A(cx) = c(Ax) = c0 = 0$$

  $\square$

- $V = \mathbb{M}_{m\times n}(\mathbb{F})$
  - $W = \{A \in M_{m\times n}(\mathbb{F}) := AT = A\}$
  - $W =$ diagonal $m \times n$ matrices
  - $W =$ space of all upper triangular matrices
  - $W = \{A \in M_n(\mathbb{F}) | tr(A) = 0\}$

Definition. Let V be a vector space over a field of scalars $\mathbb{F}$ and let S be a nonempty subset of V. We say that $v \in V$ is in the span of S, if v is a linear combination of a finite number of elements in S.

span(S) is the set of all linear combinations of vectors in S

$$\text{span}(\emptyset) = \{0\}$$

S generates V if span(S) $= V$

Definition. Let V be a vector space over $\mathbb{F}$. A subset $S \subset V$ is called linearly dependent if there is a finite number of distinct vectors $u_1, ..., u_n \in S$ and scalars $a_1, ..., a_n$, not all zero, such that

$$a_1u_1 + ... + a_nu_n = 0$$

S is linearly independent if it is not linearly dependent.

A trivial linear combination for the vector 0 would be setting all the coefficients to 0

Claim: A subset S of V is linearly independent iff the only linear combination for 0 in $span(S)$ is the trivial one.

Proof. Assume that S is linearly independent. Cannot form 0 vector using nonzero scalars for $u_1, ..., u_n \in S$. Since $span(S)$ is the set of all linear combinations of vectors in S, it must be the trivial solution. To prove the opposite direction, use the contrapositive. If $S \subset V$ is linearly dependent, then there exists a nontrivial linear combination for 0 in $span(S)$. $\square$

$Ax = 0$ has a unique solution iff the set is $\{u_1, ..., u_n\}$ (which forms A) is linearly independent.

Assume $S_1 \subseteq S_2$. If S_2 is linearly independent, then S_1 is linearly independent. If S_1 is linearly dependent, then S_2 is linearly dependent.

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

Observe:

1. $S = \emptyset$ is linearly independent. Then $\emptyset$ is a basis for $v = \{0\}$

2. $S = \{u\}$ is linearly independent if and only if $u \neq 0$

   Proof. Since S is linearly independent, we only have the trivial combination for 0. But if $u = 0$, then $1 \cdot u = 0$ would be a nontrivial combination for 0, so a contradiction. Assume that $u \neq 0$. Let $a \cdot u = 0$ because $u \neq 0$. We have $a = 0$, so no dependence exists. Therefore S is linearly independent. $\square$

3. $v = \mathcal{P}(\mathbb{R})$
   $S = \{1, x, x^2, ...\}$. S is spanning and linearly independent because $a_0 + a_1x + a_2x^2 + ... + a_nx^n = 0$ if and only if $a_0 = a_1 = ... = a_n = 0$. So, there is no dependence relations in S.

4. $P(\mathbb{R}) = \mathbb{R}^{\bigoplus \mathbb{N}}$ is the set of sequences where the tail is all zeros

5. $V = \mathbb{F}^n$
   This is the space of n-tuples with entries in $\mathbb{F}$.

$$B = \begin{cases} e_1 = (1, 0, ..., 0) \\ e_2 = (0, 1, ..., 0) \\ \vdots \\ e_n = (0, 0, ..., 1) \end{cases}$$

   We say that B is the standard basis of $\mathbb{F}$. B is spanning because any $a = (a_1, a_2, ..., a_n) = a_1e_1 + a_2e_2 + ... + a_ne_n$. B is linearly independent because $a_1e_1 + ... + a_ne_n = (0, ..., 0)$ if and only if $(a_1, a_2, ..., a_n) = (0, 0..., 0)$.

6. $V = \mathbb{R}^2$
   Let $B_1 = \{e_1, e_2\}$ and $B_2 = \{e_1 + e_2, e_1 - e_2\}$. Both are bases for V.

Proof. B_2 is spanning. $v = (a, b) = x_1v_1 + x_2v_2$ implies that $x_1 = \frac{a+b}{2}$ and $x_2 = \frac{a-b}{2}$. It is also linearly indepedent. $x_1v_1 + x_2v_2 = 0$ if and only iff $(x_1, x_2) = (0, 0)$. □

7. If $\mathbb{F}$ is an arbitrary field of scalars, then $\{e_1 + e_2, e_1 - e_2\}$ is a basis for $\mathbb{F}^2$ if and only if $char(\mathbb{F}) \neq 2$.

8. $V = P_n(\mathbb{F})$ is the set of polynomials of degree less than or equal to n with coefficients in $\mathbb{F}$

Important: Let V be a vector space over $\mathbb{F}$ and let $u_1, u_2, ..., u_n \in V$. $B = \{u_1, u_2, ..., u_n\}$ is a basis for V if and only if each $v \in V$ can be uniquely expressed as a combination of $u_1, u_2, ..., u_n$.

Proof. Assume B is a basis meaning $V = span(B)$. So, for all $v \in V$ it can be expressed as a linear combination. Assume that v can be written in two ways. $v = c_1u_1 + ... + c_nu_n = d_1u_1 + ... + d_nu_n$. $0 = v - v = (c_1 - d_1)u_1 + ... + (c_n - d_n)u_n$. Since the basis is linearly independent, we must have $c_1 = d_1, ..., c_n = d_n$. Assume that B can be uniquely expressed. Then, the only combination for 0 is the trivial solution and the vectors span V. So, B is a basis for V. □

Claim: If V is generated by a finite sets, then some subset of S is a basis for V.

Proof. If $S =$ or $S = \{0\}$. Otherwise, take some nonzero vector $u_1 \in S$. Then $\{u_1\}$ is linearly independent. If possible, choose some vectors $s_2, ... \in S$ such that the set $\{u_1, u_2, .., u_k\}$ is linearly independent for all $k \geq 1$. By finiteness of S, this process ends and we call the resulting linearly independent subset of S as $B = \{u_1, u_2, ..., u_n\}$. We claim that this B generates V. Note that either $B = S$ so B is a basis or $B \subset S$. Then $S \subset B \implies span(S) \subset span(B) \implies V = span(B)$. Therefore, B is a basis. □

Claim: (Replacement Theorem) Let V be any vector space over $\mathbb{F}$ generated by a set G containing exactly n vectors. If L is a linearly independent subset of V containing exactly m vectors, then $m \leq n$. Also there is a subset H of G containing exactly $n - m$ vectors such that $L \cup H$ generates V.

Proof. (by induction) If $m = 0$, $L = \emptyset$, then $H = G$. Next assume the statement holds for $m \geq 0$. $\mathcal{L} = \{v_1, v_2, ..., v_{m+1}\}$. Then, $\{v_1, v_2, ..., v_m\}$ is linearly independent. By IH, we know $m \leq n$ and there is a subset $\{u_1, u_2, ..., u_{n-m}\}$ of G such that $\{v_1, v_2, ..., v_m\} \cap \{u_1, u_2, ..., u_{n-m}\}$ generates V. Then, $v_{m+1} = a_1v_1 + a_2v_2 + ... + a_nv_m + b_1u_1 + ... + b_{n-m}u_{n-m}$ for some $a_i, b_j \in \mathbb{F}$. We already know $n - m \geq 0$ but we claim $n - m \neq 0$ because otherwise L would not be linearly independent. So $n \geq m + 1$ and some $b_j \neq 0$. Without loss of generality, consider $b_1 \neq 0$.

$$u_1 = \left(-\frac{a_1}{b_1}\right) v_1 + ... + \left(-\frac{a_n}{b_1}\right) v_m + \left(\frac{1}{b_1}\right) v_{m+1} + \left(-\frac{b_2}{b_1}\right) u_2 + ... + \left(-\frac{b_{n-m}}{b_1}\right) u_{n-m}$$

Let $H = \{u_2, u_3, ..., u_{n-m}\}$. Then $u_1 \in span(L \cup H)$. So, $V = span(L \cup H)$. □

Claim: Let B have a finite basis. Then all bases for B are finite and all have the same number of vectors.

Proof. Let B be a basis with cardinality of V. $|B| = n$ and let C be any other basis. If $|C| > n$, then choose a subset $S \in C$ with exactly $n + 1$ vectors. But then I have $n + 1$ linearly independent vectors in something that is spanned by n vectors, which is a contradiction so C is finite and $m \leq n$. Similarly, $n \leq m$ and $n = m$. □

Definition. Let V be any vector space over $\mathbb{F}$. We call V finite dimensional if it has a finite basis. We then call the number of vectors in any basis the dimension of V. If V is not finite dimensional, we call it infinite dimensional.

Examples:

1. $V = \{0\}$; $\dim V = 0$ because $\{\}$ is a basis
2. $F = \mathbb{C}, V = \mathbb{C}$; $\dim_{\mathbb{C}} \mathbb{C} = 1$ because $\{1\}$ is a basis
3. $F = \mathbb{R}, V = \mathbb{C}$; $\dim_{\mathbb{R}} \mathbb{C} = 2$ because $\{1, i\}$ is a basis
4. $V = P(\mathbb{F})$ is infinite dimensional

Important: A vector space always has a basis
Existence of Basis and Axiom of Choice

Proof. Take nonempty set $A_\alpha \neq \emptyset$ □

Linear Transformations

Definition. Let V and W be vector spaces over $\mathbb{F}$. A transformation $T : V \to W$ is called linear if the following hold

1. $T(x + y) = T(x) + T(y)$ for all $x, y \in V$
2. $T(cx) = cT(x)$ for all $c \in \mathbb{F}$ and $x \in \mathbb{V}$

Observe that if T is linear then

1. $T(0_V) = 0_W$
2. $T(x - y) = T(x) - T(y)$
3. $T(\sum_i c_i x_i) = \sum_i c_i T(x_i)$

Definition. Given $V, W/\mathbb{F}$ and $T : V \to W$ linear, define null space (or kernel) of T:

$$N(T) = \{x \in V : T(x) = 0\}$$

and the range (or image) of T:

$$R(T) = \{T(x) : x \in V\}$$

Example

1. $T : V \to V$ $(x \to x)$; Range is all of V, Null space is $\{0\}$
2. $T : V \to W$ $(x \to 0)$

Theorem: Let $T \in \mathcal{L}(V, W)$, then $R(T)$ is a subspace of W.
Theorem: Let $T \in \mathcal{L}(V, W)$, then $N(T)$ is a subspace of V.
Theorem: Let $T \in \mathcal{L}(V, W)$, then T is injective if and only if $N(T) = \{0\}$.

Proof. Assume that T is injective. Assume $T(v) = 0_W$. By injectivity, $v = 0_V$. So, $N(T) = \{0\}$. Assume $N(T) = \{0\}$. Take any $v_1 \neq v_2 \in V$. Assume that $T(v_1) = T(v_2)$. Then $T(v_1) - T(v_2) = T(v_1 - v_2) = 0$. ☐

Definition. Given V, W as vector spaces over $\mathbb{F}$ and a linear $T : V \to W$. If $N(T)$ and $R(T)$ are finite dimensional, then define **nullity** of T as $\dim N(T)$ and **rank** of T as $\dim R(T)$.

Rank-Nullity Theorem: If V is finite dimensional, then $\dim V =$ nullity of $T +$ rank of T.

Proof. Let $\dim V = n$ and $\dim N(T) = k$. $k \leq n$ because $N(T)$ is a subspace of V. Choose basis $\{v_1, ..., v_k\}$ for the nullspace. Extend it to B for V, where $B = \{v_1, ..., v_k, v_{k+1}, ..., v_n\}$. We claim $\{T(v_{k+1}), ..., T(v_n)\}$ is a basis for the range. T on the basis $\{v_1, ..., v_k\}$ will be 0. ☐

Example: If V and W are finite dimensional with equal dimension. For, $T : V \to W$, (a) T is injective, (b) T is surjective, and (c) rank $(T) = \dim V = \dim W$

Claim: Let V, B be vector spaces over $\mathbb{F}$. $\{v_1, ..., v_n\}$ is a basis for V. Let $w_1, ..., w_n \in W$. Then $\exists!\, T : V \to W$ such that $T(v_i) = w_i$ for all $1 \leq i \leq n$.

Proof. Existence: Define $T\left(\sum_{i=1}^n c_i v_i\right) := \sum_{i=1}^n c_i w_i$. This T defines a linear transformation $T(v_i) = w_i$.
Uniqueness: Assume there exists another $S : V \to W$ satisfying the property. Then,

$$S(v) = S\left(\sum c_i v_i\right) = \sum c_i S(v_i) = \sum c_i w_i = T\left(\sum c_i v_i\right) = T(v)$$

☐

Definition. Let V be a finite dimensional vector space over $\mathbb{F}$ and let $B = \{v_1, ..., v_n\}$ be an ordered basis for V. For any $x \in V$, write $x = \sum_{i=1}^n a_i v_i$. We define the coordinate vector of x relative to B as the following,

$$[x]_B = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

Definition. Let V be a finite dimensional vector space over $\mathbb{F}$ with an ordered basis $B = \{v_1, ..., v_n\}$ and let W be a finite dimensional vector space over $\mathbb{F}$ with an ordered basis $C = \{w_1, ..., w_m\}$. Then, the matrix of a linear transformation $T : V \to W$ is

$$A = [T]_B^C := [a_{ij}]_{m \times n} = \begin{pmatrix} [T(v_1)]_C & \cdots & [T(v_n)]_C \end{pmatrix}$$

If $V = W$ and $B = C$, then we write $[T]_B$.

The Kronecker-Delta function is

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Examples:

1. The identity transformation $Id : V \to V$. If V is finite dimensional with basis β, then $[T]_\beta = [\delta_{ij}]_{n\times n} = I$
2. $T : V \to W$, where every $v \in V$ is mapped to $0 \in W$, then $[T] = [0]_{m\times n}$
3. Isomorphism: Let V and W be vector spaces over $\mathbb{F}$. Set $\mathcal{L}(V, W) := \{$ linear transformations $V \to W\}$. $\mathcal{L}(V, W)$ is a vector space over $\mathbb{F}$. If $V = W$, we write $\mathcal{L}(V) := \mathcal{L}(V, V)$. When $\dim V = n < \infty$ and $\dim W = m < \infty$, then there is a bijection between $\mathcal{L}(V, W)$ and $M_{m\times n}(\mathbb{F})$. This is an isomorphism because

$$[T+U]_\beta^\mathcal{C} = [T]_\beta^\mathcal{C} + [U]_\beta^\mathcal{C} \quad [aT]_\beta^\mathcal{C} = a[T]_\beta^\mathcal{C}$$

Let V, W, Z be vector spaces over $\mathbb{F}$. Let $T : V \to W$ and $U : W \to Z$. Then, $UT = U \circ T = V \to Z$.

Observe:

1. $T \in \mathcal{L}(V, W)$ and $U \in \mathcal{L}(W, Z)$ implies $UT \in \mathcal{L}(V, Z)$

$$(UT)(x + y) = U(T(x + y)) = U(T(x) + T(y)) = U(T(x)) + U(T(y)) = (UT)(x) + (UT)(y)$$

$$(UT)(ax) = U(T(ax)) = U(aT(x)) = aU(T(x)) = a(UT)(x)$$

2. If $T_1, T_2 \in \mathcal{L}(V, W)$ and $U_1, U_2 \in \mathcal{L}(W, Z)$, then $U_1(T_1 + T_2) = (U_1T_1) + (U_1T_2)$ and $(U_1 + U_2)(T_1) = (U_1T_1) + (U_2T_1)$.
3. Composition is associative
4. $T \in \mathcal{L}(V, W)$ implies $T = TI_V = I_WT$
5. $a(UT) = (aU)T = U(aT)$
6. When $T \in \mathcal{L}(V)$, $T^0 = I_V, T^1 = T, T^2 = TT, T^3 = TTT, ...$
7. Assume that $T : V \to W$, $U : W \to Z$, V has basis $\mathcal{B}$, W has basis $\mathcal{C}$, and Z has basis $\mathcal{D}$. Also, $\dim V = n, \dim W = m, \dim Z = p$. So, $[T]_\mathcal{B}^\mathcal{C} = B_{m\times n}$ and $[U]_\mathcal{B}^\mathcal{D} = A_{p\times m}$. Then, $[UT]_\mathcal{B}^\mathcal{D} = C_{p\times n}$. This leads to the definition of matrix multiplication.

$$(UT)(v_j) = U(T(v_j)) = U\left(\sum_k B_{kj}w_k\right) = \sum_k B_{kj}U(w_k) = \sum_k B_{kj}\left(\sum_i A_{ik}z_i\right) = \sum_i C_{ij}z_i$$

So, $C = AB$ with $C_{ij} = A_{i1}B_{1j} + ... + A_{ip}B_{pj}$.

Examples: Properties of Matrix Multiplication: For $A_{m\times n}, B_{n\times p}, C_{n\times p}, D_{q\times m}, E_{q\times m}$ matrices,

1. $A(B + C) = (AB) + (AC) \quad (D + E)A = (DA) + (EA)$
2. $a(AB) = (aA)B = (A)(aB)$ for all $a \in \mathbb{F}$
3. $I_mA = A = A = AI_n$
4. $AB = AC \not\Longrightarrow B = C$ even if $A \neq 0$

5. Given $B = \begin{bmatrix} v_1 & v_2 & \cdots & v_p \end{bmatrix}$, $AB = \begin{bmatrix} Av_1 & Av_2 & \cdots & Av_p \end{bmatrix}$

6. Let V and W be finite dimensional vector space over $\mathbb{F}$ with bases $\mathcal{B}$ and $\mathcal{C}$. Let $T : V \to W$ be a linear transformation. Then,

$$[T(u)]_{\mathcal{C}} = [T]_{\mathcal{B}}^{\mathcal{C}}[u]_{\mathcal{B}}$$

7. Fix $A_{m\times n}$, define $L_A : \mathbb{F}^n \to \mathbb{F}^m$ via $L_A(x) = Ax$ (left multiplication). Consider $\mathcal{B}$ and $\mathcal{C}$ standard bases of $\mathbb{F}^n$ and $\mathbb{F}^m$ respectively. Then,
   (a) $[LA]_{\mathcal{B}}^{\mathcal{C}} = A$
   (b) $L_A = L_B \iff A = B$
   (c) $L_{A+B} = L_A + L_B$
   (d) For $T : \mathbb{F}^n \to \mathbb{F}^m$, there exists a unique C such that $T = L_C$
   (e) Given E, we have $L_{AE} = L_A L_E$
   (f) When $m = n$, we have $L_{I_n} = I_{\mathbb{F}^n}$
   (g) Upshot: Left mulitplication transformations from $\mathbb{F}^n$ to $\mathbb{F}^m$ is an isomorphism to $m \times n$ matrices