MATH405: Linear Algebra

Michael Li

Contents

1 Vector Spaces **2**
- 1.1 Definitions . . . 2
- 1.2 Bases . . . 4
- 1.3 Dimension . . . 6
- 1.4 Sums and Direct Sums . . . 8

2 Matrices **9**
- 2.1 Space of Matrices . . . 9
- 2.2 Linear Equations . . . 10
- 2.3 Multiplication of Matrices . . . 11

1 Vector Spaces

1.1 Definitions

Definition - Field: Let K be a subset of C. Then K is a **field** if it satisfies

1. $x, y \in K \implies x + y, xy \in K$
2. $x \in K \implies -x \in K$ and $x \in K, x \neq 0 \implies x^{-1} \in K$
3. $0, 1 \in K$

Definition - Scalars: elements of a field K

Definition - Subfield: Let K, L be fields and $K \subseteq L$. Then K is a **subfield** of L

- **Example**: Q is a subfield of R which is a subfield of C

Definition - Vector Space V Over the Field K: set of objects that can be added and multiplied by elements of K such that

- $u, v \in V \implies u + v \in V$
- $c \in K$ and $v \in V \implies cv \in V$

A vector space also satisfies the following properties for $u, v, w \in V$ and $a, b \in K$:

- **Commutativity**: $u + v = v + u$
- **Associativity**: $(u + v) + w = u + (v + w)$ and $(ab)v = a(bv)$
- **Additive Identity**: $\exists O \in V$ such that $v + O = v$ for all $v \in V$
- **Additive Inverse**: $\forall v \in V, \exists w \in V$ such that $v + w = O$
- **Multiplicative Identity**: $1v = v$ for all $v \in V$
- **Distributive Properties**: $a(u + v) = au + av$ and $(a + b)v = av + bv$

Example: Let $V = K^n$ be the set of n-tuples of elements of K. Then

$$A = (a_1, \ldots, a_n) \qquad B = (b_1, \ldots, b_n)$$

are elements of K^n

Here $a_1, \ldots, a_n$ are called **components** of A

Furthermore, defining

- **Addition** as $A + B = (a_1 + b_1, \ldots, a_n + b_n)$
- **Scalar Multiplication** as $cA = (ca_1, \ldots, ca_n)$

We see that K^n clearly satisfies the properties of a vector space

- Notably, the zero element is the n-tuple with all coordinates equal to 0

$$O = (0, \ldots, 0)$$

Few more notes on any vector space V

- For any $v \in V$, we have $0v = O$

$$0v + v = (0 + 1)v = 1v = v \implies 0v = O$$

Definition - Subspace: Let $W \subseteq V$. Then W is a **subspace** if it satisfies

1. $u, w \in W \implies u + w \in W$
2. $c \in K$ and $v \in W \implies cv \in W$
3. $O \in W$

Example: Let $V = K^n$ and W be a set of $v \in V$ with the last coordinate equal to 0. Then W is a subspace of V

Definition - Linear Combination: Let V be an arbitrary vector space, and take $v_1, \dots, v_n \in V$ and $x_1, \dots, x_n \in K$. Then expressions of the form

$$x_1 v_1 + \cdots + x_n v_n$$

are called **linear combininations** of $v_1, \dots, v_n$

Theorem 1.1: Let W be a set of all linear combinations of $v_1, \dots, v_n$. Then W is a subspace of V

Proof: Take $x_1, \dots, x_n, y_1, \dots, y_n \in K$. Then we have

$$(x_1 v_1 + \cdots + x_n v_n) + (y_1 v_1 + \cdots + y_n v_n) = (x_1 + y_1)v_1 + \cdots + (x_n + y_n)v_n \in W$$

Furthermore, take $c \in K$. Then we have

$$(cx_1 v_1 + \cdots + x_n v_n) = cx_1 v_1 + \cdots cx_n v_n \in W$$

Finally, we see that

$$O = 0v_1 + \cdots + 0v_n \in W$$

- **Note**: The subspace created above is called the subspace **generated** by $v_1, \dots, v_n$

Example: Let $V = K^n$ and let $A, B \in K^n$. Then we define the **dot product** as

$$A \cdot B = a_1 b_1 + \cdots + a_n b_n$$

The following properties hold

1. $A \cdot B = B \cdot A$
2. $A \cdot (B + C) = A \cdot B + A \cdot C = (B + C) \cdot A$
3. $x \in K \implies (xA) \cdot B = x(A \cdot B)$ and $A \cdot (xB) = x(A \cdot B)$

Proof:

1. $a_1 b_1 + \cdots + a_n b_n = b_1 a_1 + \cdots b_n a_n$
2. $A \cdot (B + C) = a_1(b_1 + c_1) + \cdots + a_n(b_n + c_n) = a_1 b_1 + \cdots a_n b_n + a_1 c_1 + \cdots a_n b_n = A \cdot B + A \cdot C$

Definition - Orthogonal: Two vectors A, B are **orthogonal** if $A \cdot B = 0$

- If we look at W, the set of all elements $B \in K^n$ such that $B \cdot A = 0$, we see that W is a subspace of K^n
  - Clearly $O \cdot A = 0 \implies O \in W$
  - $B, C \in W \implies (B + C) \cdot A = B \cdot A + C \cdot A = 0 \implies B + C \in W$
  - $x \in K \implies (xB) \cdot A = x(B \cdot A) = 0 \implies xB \in A$

Example - Function Spaces: Let S be a set and K be a field. Then a **function** S into K is an association between $s \in S$ and a unique $k \in K$. The function f is denoted

$$f : S \to K$$

Let V be the set of all functions S into K. We define

- **Addition** as $f, g \in S \implies (f + g)(x) = f(x) + g(x)$ for $x \in S$
- **Scalar Multiplication** as $c \in K \implies (cf)(x) = cf(x)$ for $x \in S$

Under this definition, V is a vector space

Example: Let V be a vector space and let U, W be subspaces of V. Then $U \cap W$ is a subspace of V

Example - Sum of Subspaces: Let U, W be subspaces of V. Then

$$U + W = \{u + w \mid u \in U \wedge w \in W\}$$

is a subspace of V known as the **sum** of U and W

1.2 Bases

Definition - Linearly Dependent: $v_1, \ldots, v_n \in V$ are **linearly dependent** over K if $\exists a_1, \ldots, a_n \in K$ not all 0 such that

$$a_1 v_1 + \cdots a_n v_n = O$$

- If no such numbers exist, then $v_1, \ldots, v_n$ are **linearly independent**

Example: Let $V = K^n$ and consider

$$E_1 = (1, 0, \ldots, 0)$$
$$\vdots$$
$$E_n = (0, 0, \ldots, 1)$$

Then $E_1, \ldots, E_n$ are linearly independent since

$$a_1 E_1 + \cdots + a_n E_n = O \implies (a_1, \ldots, a_n) = O \implies a_i = 0$$

Definition - Basis: If $v_1, \ldots v_n \in V$ generate V and are linearly independent, then $\{v_1, \ldots, v_n\}$ is a **basis** of V

- **Example**: $E_1, \ldots, E_n$ from the previous example form a basis of K^n

Theorem 2.1: Let V be a vector space, $v_1, \ldots v_n \in V$ be linearly independent, and $x_1, \ldots, x_n, y_1, \ldots, y_n \in K$. Then we have

$$x_1 v_1 + \cdots + x_n v_n = y_1 v_1 + \cdots + y_n v_n \implies x_i = y_i$$

Proof: We can manipulate the equation above into

$$x_1 v_1 - y_1 v_1 + \cdots + x_n v_n - y_n v_n = (x_1 - y_1) v_1 + \cdots + (x_n - y_n) v_n = O$$

Thus we must have $x_i - y_i = 0 \implies x_i = y_i$

Upshot: If $\{v_1, \ldots, v_n\}$ is a basis of V, then elements of V can be represented by n-tuples relative to this basis as a LC

$$v = x_1 v_1 + \cdots + x_n v_n$$

Thus each n-tuple $(x_1, \ldots, x_n)$ is uniquely determined by v

Definition - Coordinate Vector: The tuple above $X = (x_1, \ldots, x_n)$ is a **coordinate vector** of v with respect to the basis $\{v_1, \ldots, v_n\}$

Example: Suppose V is the vector space of functions generated by e^t, e^{2t}. Then coordinates of the function

$$3e^t + 5e^{2t}$$

with respect to the basis $\{e^t, e^{2t}\}$ are $(3, 5)$

Example: Show that $(1, 1)$ and $(-3, 2)$ are linearly independent

Take $a, b \in K$ such that

$$a(1, 1) + b(-3, 2) = O$$

In terms of components, this means we need

$$a - 3b = 0 \qquad a + 2b = 0$$

The only way to solve this system of equation is to take $a = b = 0$

Thus the vectors are linearly independent

Example: Show that $(1, 1)$ and $(-1, 2)$ form a basis of R^2

We need to show they are linearly independent and that they generate R^2

To show linear independence, we need $a, b \in R$ such that

$$a(1, 1) + b(-1, 2) = (0, 0) \implies a - b = 0 \qquad a + 2b = 0$$

The only way to solve this system of equations is taking $a = b = 0$

To show the vectors generate R^2, let (a, b) be an arbitrary element of R^2. Then there exists $x, u \in R$ such that

$$x(1, 1) + y(-1, 2) = (a, b) \implies x - y = a \qquad x + 2y = b$$

Solving the system of equations we get

$$y = \frac{b - a}{3} \qquad x = \frac{b - a}{3} + a$$

Thus we have shown that (x, y) are the coordinates of (a, b) with respect to the basis $\{(1, 1), (-1, 2)\}$

Definition - Maximal: Let $\{v_1, \ldots, v_n\}$ be a set of elements of V. For $r \leq n$, $\{v_1, \ldots, v_r\}$ is a **maximal** subset of linearly independent elements if $v_1, \ldots, v_r$ are linearly independent, and if in addition, given any v_i for $i > r$, $v_1, \ldots, v_r, v_i$ are linearly dependent

Theorem 2.2: Let $\{v_1, \ldots, v_n\}$ be a set of generators of V, and let $\{v_1, \ldots, v_r\}$ be a maximal subset of linearly independent elements. Then $\{v_1, \ldots, v_r\}$ is a basis of V

Proof: We need to show that $v_1, \ldots, v_r$ generate V.

First we show that for $i > r$, each v_i is a linear combination of $v_1, \ldots, v_r$. Since $v_1, \ldots, v_r, v_i$ is linearly dependent, there exists $x_1, \ldots, x_r, y$ not all 0 such that

$$x_1 v_1 + \cdots + x_r v_r + y v_i = O$$

We must have $y \neq 0$, otherwise $v_1, \ldots, v_r$ would be linearly dependent. Thus we can solve for v_i

$$v_i = \frac{x_1}{-y} v_1 + \cdots + \frac{x_r}{-y} v_r$$

Thus v_i is a linear combination of $v_1, \ldots, v_r$

Next we show that for any of $v \in V$, there exists $c_1, \ldots, c_n \in K$ such that

$$v = c_1 v_1 + \cdots + c_n v_n$$

From this equation, we can replace each v_i, for $i > r$, by a linear combination of $v_1, \ldots, v_r$.

Collecting the terms with the representation, we have expressed v as a linear combination of $v_1, \ldots, v_r$

Thus $v_1, \ldots, v_r$ generate V and thus is a basis of V

1.3 Dimension

Theorem 3.1: Let $\{v_1, \ldots, v_m\}$ be a basis of V over K. Let $w_1, \ldots, w_n$ be elements of V and assume $n > m$. Then $w_1, \ldots, w_n$ are linearly dependent

Proof: Assume by contradiction that $w_1, \ldots, w_n$ are linearly independent

Since $\{v_1, \ldots, v_m\}$ is a basis, there are elements $a_1, \ldots, a_m \in K$ such that

$$w_1 = a_1 v_1 + \cdots + a_m v_m$$

Since we are assuming $w_1, \ldots, w_n$ are linearly independent, we must have $w_1 \neq O \implies$ some $a_i \neq 0$

After some reordering of $v_1, \ldots, v_m$, WLOG $a_1 \neq 0$. Solving for v_1 we get

$$\begin{aligned} a_1 v_1 &= w_1 - a_2 v_2 - \cdots - a_m v_m \\ v_1 &= a_1^{-1} w_1 - a_1^{-1} a_2 v_2 - \cdots - a_1^{-1} a_m v_m \end{aligned}$$

Thus the subspace of V generated by $w_1, v_2, \ldots, v_m$ contains v_1. Thus the subspace must be all of V since $v_1, \ldots, v_m$ generate V

We can continue this procedure replacing $v_2, v_3, \ldots$ with $w_2, w_3, \ldots$ until all $v_1, \ldots, v_m$ are exhausted and $w_1, \ldots, w_m$ generate V

Now assume by induction that there is an integer r with $1 \leq r < m$ such that after renumbering $v_1, \ldots, v_m$ the elements $w_1, \ldots, w_r, v_{r+1}, \ldots, v_m$ generate V. Then there are $b_1, \ldots b_r, c_{r+1}, \ldots, c_m \in K$ such that

$$w_{r+1} = b_1 w_1 + \cdots + b_r w_r + c_{r+1} v_{r+1} + \cdots + c_m v_m$$

Note that some $c_i \neq 0$ for $i \in \{r+1, \ldots, m\}$, otherwise $w_1, \ldots, w_r$ would be linear dependent

Thus WLOG we can say $c_{r+1} \neq 0$ and can obtain

$$c_{r+1} v_{r+1} = w_{r+1} - b_1 w_1 - \cdots - b_r w_r - c_{r+2} v_{r+2} - \cdots - c_m v_m$$

Thus v_{r+1} is in the subspace generated by $w_1, \ldots, w_{r+1}, v_{r+2}, \ldots, v_m$.

By our induction assumption, it follows that $w_1, \ldots, w_{r+1}, v_{r+2}, \ldots, v_m$ generate V

Thus by induction, we have shown that $w_1, \ldots, w_m$ generate V

If $n > m$, then there exist elements $d_1, \ldots, d_m \in K$ such that

$$w_n = d_1 w_1 + \cdots + d_m w_m$$

Thus $w_1, \ldots, w_n$ are linearly dependent

Theorem 3.2: Let V be a vector space and suppose that one basis has n elements and another basis has m elements. Then $m = n$

Proof: Theorem 3.1 implies that both $n > m$ and $m > n$ are impossible. Thus we must have $m = n$

Definition - Dimension: Let V be a vector space having a basis with n elements. Then n is the **dimension** of V

- **Note**: If V only consists of O, then V doesn't have a basis and thus $\dim V = 0$

Example: For any field K, the vector space K^n has dimension n over K since

$$(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 0, 1)$$

form a basis of K^n over K

Definition - Finite Dimensional: A vector space that has a basis consisting of a finite number of elements, or the zero vector space

- Otherwise the vector space is **infinite dimensional**

Example: Let K be a field. Then K is a vector space over itself and has dimension 1

- The element $1 \in K$ forms a basis of K over K since for any $x \in K$, $x = x \cdot 1$

Example: Let V be a vector space.

- A subspace of dimension 1 is called a **line**
- A subspace of dimension 2 is called a **plane**

Definition - Maximal Set of Linearly Independent Elements: linearly independent $v_1, \ldots, v_n \in V$ such that for any $w \in V$, the elements $w, v_1, \ldots, v_n$ are linearly dependent

Theorem 3.3: Let $\{v_1, \ldots, v_n\}$ be a maximal set of linearly independent elements of V. Then $\{v_1, \ldots, v_n\}$ is a basis of V

Proof: We need to show that $v_1, \ldots, v_n$ generates V

Let $w \in V$. Since $w, v_1, \ldots, v_n$ is linearly dependent, there exists numbers $x_0, \ldots, x_n$ not all 0 such that

$$x_0 w + x_1 v_1 + \cdots + x_n v_n = O$$

We must have $x_0 \neq 0$, otherwise there would be a linear dependence between $v_1, \ldots, v_n$. Thus we can solve for w

$$w = -\frac{x_1}{x_0} v_1 - \cdots - \frac{x_n}{x_0} v_n$$

Thus w is a linear combination of $v_1, \ldots, v_n$ and thus $\{v_1, \ldots, v_n\}$ is a basis

Theorem 3.4: Let V be a vector space of dimension n and $v_1, \ldots, v_n$ be linearly independent. Then $\{v_1, \ldots, v_n\}$ is a basis of V

Proof: By Theorem 3.1, we know that $v_1, \ldots, v_n$ is a maximal set of linearly independent elements of V

Thus by Theorem 3.3, it is a basis

Corollary 3.5: Let W be a subspace of a vector space V. If $\dim W = \dim V$, then $V = W$

Proof: From Theorem 3.4, we see that W must also be a basis of V

Corollary 3.6: Let V be a vector space of dimension n, take $r < n$, and let $v_1, \ldots, v_r$ be linearly independent. Then one can find elements $v_{r+1}, \ldots, v_n$ such that

$$\{v_1, \ldots, v_n\}$$

is a basis of V

Proof: Since $r < n$, $\{v_1, \ldots, v_r\}$ cannot form a basis of V and thus is not a maximal set of linearly independent elements of V

Thus we can find $v_{r+1} \in V$ such that $v_1, \ldots, v_{r+1}$ are linearly independent

We can repeat this process so long as $r + 1 < n$

Afterwards, we obtain n linearly independent elements, which by Theorem 3.4 form a basis

Theorem 3.7: Let V be a vector space with a basis of n elements. Let W be a subspace which does not consist of only O. Then W has a basis and $\dim W \leq n$

Proof: Let w_1 be a non-zero element of W. If $\{w_1\}$ is not a maximal set of linearly independent elements of W, we can find another element $w_2 \in W$ such that w_1, w_2 are linearly independent

Repeat this procedure until we have $m \leq n$ such that $w_1, \ldots, w_m$ form a maximal set of linearly independent elements of W

- By Theorem 3.1, we know that this procedure cannot go on indefinitely

Thus using Theorem 3.3, we see that $\{w_1, \ldots, w_m\}$ is a basis of W

1.4 Sums and Direct Sums

Definition - Sum: Let U, W be subspaces of V. Then the **sum** of $U + W$ is a subset of V consisting of all sums $u + w$ for $u \in U$ and $w \in W$

- $U + W$ is a subspace since it is closed under addition, scalar multiplication, and contains O

Definition - Direct Sum: V is a **direct sum** of U and W, denoted $V = U \oplus W$, if for every element of V, there exists unique elements $u \in U$ and $w \in W$ such that $v = u + w$

Theorem 4.1: Let U, W be subspaces of V. If $U + W = V$ and $U \cap V = \{O\}$, then V is a direct sum of U and W

Proof: Take $v \in V$. The first assumption shows that $\exists u \in U \wedge w \in W$ such that $v = u + w$. Thus $V = U + W$

To show it is a direct sum, we need to show that u, w are unique.

Assume by contradiction that there also exists $u' \in U$ and $w' \in W$ such that $v = u' + w'$

Then we have

$$u + w = u' + w' \implies u - u' = w' - w$$

Since $u - u' \in U$ and $w' - w \in W$, and since $U \cap W = \{O\}$, we must have $u - u' = O$ and $w' - w = O \implies u = u'$ and $w = w'$

Theorem 4.2: Let W be a subspace of V. Then there exists a subspace U such that $V = W \oplus U$

Proof: Select a basis of W and extend it to a basis of V using Corollary 3.6

Here the basis of W is $\{v_1, \ldots, v_r\}$ and the basis of U is $\{v_{r+1}, \ldots, v_n\}$

Theorem 4.3: Let V be the direct sum of subspaces U, W. Then

$$\dim V = \dim U + \dim W$$

Proof: Let $\{u_1, \ldots, u_r\}$ be a basis of U and let $\{w_1, \ldots, w_s\}$ be a basis of W

Then every element of U has a unique representation as a linear combination of $x_1u_1 + \cdots x_ru_r$ for $x_i \in K$

Similarly, every element of W has a unique representation as a linear combination of $y_1w_1 + \cdots + y_sw_s$ for $y_j \in K$

Thus by definition, every element of V has a unique representation as a linear combination of

$$x_1u_1 + \cdots + x_ru_r + y_1w_1 + \cdots + y_sw_s$$

Clearly $u_1, \ldots, u_r, w_1, \ldots, w_s$ are linearly independent and generate V. Thus they form a basis of V

Thus we have $\dim V = \dim U + \dim W$

Definition - Direct Product: Let U, W be arbitrary vector spaces. Then the **direct product** of U and W, denoted $U \times W$, is the set of all pairs (u, w) whose first component is $u \in U$ and whose second component is $w \in W$

- Addition is defined componentwise
$$(u_1, w_1) + (u_2, w_2) = (u_1 + u_2, w_1 + w_2)$$
- Scalar multiplication is defined by
$$c(u_1, w_1) = (cu_1, cw_1)$$
- **Note**: If $n = r + s$, then we see that K^n is the direct product $K^r \times K^s$

Theorem 4.4: $\dim(U \times W) = \dim U + \dim W$

Proof: Let $\{u_1, \ldots, u_r\}$ be a basis of U and let $\{w_1, \ldots, w_s\}$ be a basis of W

Then every element of U has a unique representation as a linear combination of $x_1u_1 + \cdots x_ru_r$ for $x_i \in K$

Similarly, every element of W has a unique representation as a linear combination of $y_1w_1 + \cdots + y_sw_s$ for $y_j \in K$

Thus by definition, every element of $U \times W$ has a unique representation as a linear combination of

$$(x_1u_1 + \cdots + x_ru_r, y_1w_1 + \cdots + y_sw_s)$$

Thus the vectors form a basis and $\dim(U \times W) = \dim U + \dim W$

Note: The definition of direct sums and direct products can be extended to several elements

2 Matrices

2.1 Space of Matrices

Definition - Matrix: An m-by-n **matrix** in K is denoted by

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \cdots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

- Each **component** is denoted a_{ij} for $i = 1, \ldots, m$ and $j = i, \ldots, n$
- Each ith **row** is denoted $A_i = (a_{i1}, \ldots, a_{in})$
- Each jth column is denoted $A^j = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix}$
- **Upshot**: rows of a matrix may be viewed as n-tuples and columns may be viewed as m-tuples

Definition - Vector: $1 \times n$ matrix denoted $(x_1, \ldots, v_n)$

Definition - Column Vector: $n \times 1$ matrix denoted $\begin{bmatrix} x_1 \\ \vdots \\ v_n \end{bmatrix}$

Matrix operations:

- **Addition**: components a_{ij} and b_{ij} are added componentwise
- **Scalar Multiplication**: Each component a_{ij} is multiplied by c

Under these operations, it's clear that matrices satisfy all the properties of a vector space, which we denote $\text{Mat}_{x \times n}(K)$

Definition - Transpose: Takes an m-by-n matrix A and creates an n-by-m matrix where $b_{ji} = a_{ij}$, denoted A^t

- Taking the transpose matrix effectively changes rows into columns and vice versa

Definition - Symmetric: Matrix A is **symmetric** if it is equal to its transpose

Definition - Diagonal Matrix: A square matrix is said to be a **diagonal matrix** if all of its components are zero except possibly the diagonal components $a_{11}, \ldots, a_{nn}$

Definition - Unit Matrix: A square matrix is said to be a **unit matrix** if all of its components equal 0 except the diagonal components, which are all equal to 1. This is denoted I_n

2.2 Linear Equations

Definition - Linear Equations: Let K be a field, let A be an m-by-n matrix, and let $b_1, \dots b_m \in K$. Then linear equations are of the form

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ &\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

- This system is said to be **homogeneous** if $b_1 = \cdots = b_m = 0$
- Here the matrix A is called the **matrix of coefficients**

Clearly the homogeneous system always has the **trivial solution** where $x_j = 0$

Otherwise **non-trival solutions** are solutions $(x_1, \dots, x_n)$ such that some $x_i \neq 0$

The homogeneous system can also be rewritten as

$$x_1 \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix} + \cdots + x_n \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix} = 0$$

Thus a non-trivial solution $X = (x_1, \dots, x_n)$ is just an n-tuple $X \neq 0$, giving a relation of linear dependence between the columns $A^1, \dots, A^n$

This particular interpretation allows us to apply Theorem 3.1 of Chapter 1 where the column vectors are elements of K^m with dimension m over K

Theorem 2.1: Let

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0 \end{aligned}$$

be a homogeneous system of m linear equations in n unknowns, with coefficients in K. Assume $n > m$. Then the system has a non-trivial solution in K

Proof: By Theorem 3.1 of Chapter 1, we know that vectors $A^1, \dots, A^n$ must be linearly dependent

The general linear system of equations can be written as a linear combination of column vectors of A

$$x_1A^1 + \cdots + x_nA^n = B$$

Theorem 2.2: Assume that $m = n$ in the linear system described above, and that vectors $A^1, \dots, A^n$ are linearly independent. Then the system has a unique solution in K

Proof: Since $A^1, \dots, A^n$ are linearly independent, they form a basis of K^n

Thus any vector B has a unique expression as a linear combination of $A^1, \dots, A^n$

$$B = x_iA^1 + \cdots + x_nA^n$$

Thus $X = (x_1, \dots, x_n)$, for $x_i \in K$, is the unique solution of the system

2.3 Multiplication of Matrices

Definition - Non-degeneracy: If $A \in K^n$ and $A \cdot X = 0$ for all $X \in K^n$, then $A = O$

Proof: $A \cdot E_i = 0$ for each unit vector. Since $A \cdot E_i = a_i$, we must have each $a_i = 0$. Thus $A = O$

Definition - Matrix Product: Let A be an m-by-n matrix and B be an n-by-s matrix. Then the **product** AB is the m-by-s matrix whose ik-coordinate is

$$\sum_{j=1}^{n} a_{ij}b_{jk} = a_{i1}b_{ik} + \cdots + a_{in}b_{nk}$$

We can also interpret this definition as the dot product of row vectors, $A_1, \ldots, A_m$, of matrix A with the column vectors, $B^1, \ldots, B^s$, of matrix B. Then

$$AB = \begin{bmatrix} A_1 \cdot B^1 & \cdots & A_1 \cdot B^s \\ \vdots & \vdots & \vdots \\ A_m \cdot B^1 & \cdots & A_m \cdot B^s \end{bmatrix}$$

- For a column vector B, the product AB produces a column vector

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} c_1 \\ \vdots \\ c_m \end{bmatrix}$$

- For a row vector X, the product XA produces a row vector

$$\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} = \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix}$$

Theorem 3.1: Let A, B, C be matrices and assume that A, B can be multiplied, A, C can be multiplied, and B, C can be added. Then $A, B + C$ can be multiplied. Thus

$$A(B + C) = AB + AC$$

Furthermore, if $x \in K$, then

$$A(xB) + x(AB)$$

Proof: Let A_i be the i-th row of A, and let B^k, C^k be the k-th column of B and C, respectively

Then $B^k + C^k$ is the k-th column of $B + C$

By definition, the ik-component of AB is $A_i \cdot B^k$, the ik-component of AC is $A_i \cdot C^k$, and the ik-component of $A(B + C)$ is $A_i \cdot (B^k + C^k)$

Thus by construction we see that $A(B + C) = AB + AC$

For the second assertion, note that the k-th column of xB is xB^k

Thus we see that

$$A_i \cdot xB^k = x(A_iB^k)$$

Thus by construction, our second assertion holds

Theorem 3.2: Let A, B, C be matrices such that A, B can be multiplied and B, C can be multiplied. Then we have

$$(AB)C = A(BC)$$

Proof: TODO

Definition - Invertible: Let A be a square $n \times n$ matrix. Then A is **invertible** if there exists an $n \times n$ matrix A^{-1} such that

$$AA^{-1} = A^{-1}A = I_n$$

- **Note**: the matrix B is unique, for if there was a matrix C such that $AC = CA = I_n$, then

$$B = BI_nB(AC) + I_nC = C$$

Definition - Matrix Powers: Let A be a square matrix. Then we can form the product A with itself multiple times, denoted A^m

- The usual rule $A^{r+s} = A^rA^s$ holds for $r, s \in Z \wedge r, s \geq 0$
- *Note**: We define $A^0 = I$

Theorem 3.3: Let A, B be matrices that can be multiplied. Then B^t, A^t can be multiplied and

$$(AB)^t = B^tA^t$$

Proof: Let $A = (a_{ij})$ and $B = (b_{jk})$, and let $AB = C$. Then

$$c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}$$

Let $B^t = (b'_{kj})$ and $A^t = (a'_{ji})$. Then the ki-component of B^tA^t is defined as

$$\sum_{j=1}^{n} b'_{kj}a'_{ji}$$

Since $b'_{kj} = b_{jk}$ and $a'_{ji} = a_{ij}$, we see that

$$\sum_{j=1}^{n} b'_{kj}a'_{ji} = \sum_{j=1}^{n} a_{ij}b_{jk}$$

By definition, this is the ki-component of C^t. Thus by construction the statement holds

Upshot: In terms of matrix multiplication, we can now write a system of linear equations in the from

$$AX = B$$

For an m-by-n matrix A, a column vector X of size n, and a column vector B of size m