

Chapter 1: Fields and Polynomials

Definition 1 – Field

A field \mathbb{F} is a set with two special elements " $0 \in \mathbb{F}$ " and " $1 \in \mathbb{F}$ " and two operations " $+$ " and " \cdot " which satisfy the following axioms.

- 1) (Commutativity) For all $x, y \in \mathbb{F}$ we have: $x + y = y + x$ and $x \cdot y = y \cdot x$.
- 2) (Associativity) For all $x, y, z \in \mathbb{F}$ we have: $(x + y) + z = x + (y + z)$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- 3) (Distributivity) For all $x, y, z \in \mathbb{F}$ we have: $x \cdot (y + z) = x \cdot y + x \cdot z$.
- 4) (Identities) For all $x \in \mathbb{F}$ we have: $x + 0 = x$ and $x \cdot 1 = x$.
- 5) (Inverses) For all $x \in \mathbb{F}$ there exists $y \in \mathbb{F}$ such that $x + y = 0$. For all $x \in \mathbb{F} \setminus \{0\}$ there exists $z \in \mathbb{F}$ such that $x \cdot z = 1$.

\mathbb{Q} is a field where \mathbb{Z} is not a field because of the absence of some multiplicative inverse.

Corollary 1 – Field

Let \mathbb{F} be a field and $a, b, c \in \mathbb{F}$.

- 1) If $a + c = b + c$, then $a = b$.
- 2) If $c \neq 0$ and $c \cdot a = c \cdot b$, then $a = b$.
- 3) The field elements $0, 1$ are unique.
- 4) The elements y and z from Axiom 5 are unique. (From now on, we will denote the additive inverse of x by $-x$, and the multiplicative inverse of x by x^{-1} .)
- 5) $a \cdot 0 = 0$.
- 6) $(-a) \cdot (b) = -(a \cdot b) = (a) \cdot (-b)$.
- 7) $-(-a) = a$. If $a \neq 0$, then $(a^{-1})^{-1} = a$.
- 8) If $a \cdot b = 0$, then $a = 0$ or $b = 0$.

Theorem 1 – Equivalence

- 1) \sim is an equivalence relation.
- 2) $a \sim b$ if and only if a and b have the same remainder when divided by n .
- 3) There are exactly n equivalence classes for this relation: $[0], [1], \dots, [n-1]$ - one for each possible remainder for division by n .

Definition 2 – \mathbb{Z}_n

Let $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$ be the set of equivalence classes for this equivalence relation. We define $+, \cdot$ on \mathbb{Z}_n as follows:

$$\begin{aligned}[a] + [b] &= [a + b], \\ [a] \cdot [b] &= [a \cdot b].\end{aligned}$$

Theorem 2 – Quadratic Formula

Let $a, b, c \in \mathbb{R}$. The quadratic equation $ax^2 + bx + c = 0$ (where $a \neq 0$) has:

- 1) Solutions $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ if $b^2 - 4ac \geq 0$.
- 2) No solutions if $b^2 - 4ac < 0$.

Definition 3 – Complex

Let $i = \sqrt{-1}$. I.e. i is a number with the property that $i^2 = -1$.

Let $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. We call \mathbb{C} the set of complex numbers and we define addition and multiplication $+$, \cdot in the obvious ways:

$$(x + yi) + (a + bi) = (x + a) + (y + b)i$$

$$(x + yi) \cdot (a + bi) = ax + bi + ayi + byi^2 = (ax - by) + (ay + bx)i$$

\mathbb{C} is a field.

Given a complex number $z = x + yi$, we define its **conjugate** by:

$$\bar{z} = x - yi.$$

We define the **length (or modulus)** of a complex number by:

$$|z| = \sqrt{x^2 + y^2}.$$

Note that we in the xy -plane, we obtain \bar{z} , the conjugate of z , by reflecting z in the x -axis, and the length of a complex number is just the usual distance from z to the origin in the xy -plane.

Theorem 3 – Complex

For any $z, w \in \mathbb{C}$ we have:

- 1) $\overline{z + w} = \bar{z} + \bar{w}$.
- 2) $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$.
- 3) $\overline{\frac{z}{w}} = \frac{\bar{z}}{\bar{w}}$ (provided $w \neq 0$).
- 4) $\overline{\bar{z}} = z$.
- 5) $z\bar{z} = |z|^2$.
- 6) $z^{-1} = \frac{\bar{z}}{|z|^2}$ (provided $z \neq 0$).
- 7) $|zw| = |z||w|$.
- 8) $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$ (provided $w \neq 0$).
- 9) $|z + w| \leq |z| + |w|$ ("Triangle nequality for Complex Numbers").

Definition 4 – Polar Form

For $z = x + yi$, we define its **polar form** as $z = re^{i\theta}$, where $r = |z| = \sqrt{x^2 + y^2}$ and θ is the angle between z and the positive x axis (measured counterclockwise, in radians). The angle θ is called the **argument** of z , and r is called the **length (or modulus)** of z .

Theorem 4 – Polar Form

Let $z = re^{i\theta}$, $w = Re^{i\phi}$.

$$zw = rRe^{i(\theta+\phi)}$$

$$z^n = r^n e^{in\theta}$$

Definition 5 – Polynomial

A polynomial p with coefficient from \mathbb{F} is an expression

$$p(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$$

where $c_i \in \mathbb{F}$. We call the field elements c_0, \dots, c_n the "coefficients" of p .

The largest exponent n so that $c_n \neq 0$ is called the **degree** of p , and we typically write $\deg p = n$.

Constant polynomials are degree 0.

The set of all polynomials over \mathbb{F} is denoted by $P(\mathbb{F})$.

The set of all polynomials of degree **less than or equal** to n is denoted by $P_n(\mathbb{F})$.

Theorem 5 – Polynomial

Let \mathbb{F} be a field, and $f, g \in P(\mathbb{F})$ be non-zero polynomials. Then there exist unique polynomials $q, r \in P(\mathbb{F})$ so that:

- 1) $f(x) = q(x)g(x) + r(x)$.
- 2) $\deg r < \deg g$ if $\deg g \neq 0$.
- 3) $r = 0$ if $\deg g = 0$.

Definition 6 – Polynomial Cont.

Let \mathbb{F} be a field and $f, g \in P(\mathbb{F})$. We say that g divides f if $f(x) = q(x)g(x)$ for some polynomial $q \in P(\mathbb{F})$.

We say that a non-constant polynomial $p \in P(\mathbb{F})$ is "irreducible" if we **cannot** express p as a product of polynomials of smaller degree.

I.e. p is irreducible if we **cannot** write $p(x) = g(x)q(x)$ for any polynomials $g, q \in P(\mathbb{F})$ with the property that both $\deg g, \deg q < \deg p$.

$$f(x) = x^2 - 2 \text{ is irreducible over } \mathbb{Q} \text{ but not over } \mathbb{R}.$$

Theorem 6 – Polynomial Cont.

Let \mathbb{F} be a field, $p \in P(\mathbb{F})$ and $\deg p \geq 1$. Then $a \in \mathbb{F}$ is a root of p if and only if $x - a$ divides p .

Theorem 7 – Fundamental Theorem of Algebra

Every non-constant polynomial has a root over \mathbb{C} .

In fact, every non-constant polynomial factors completely into a product of linear terms over \mathbb{C} .

Chapter 2: Linear Systems

Definition 9 – Linear

Let \mathbb{F} be a field and $b, c_1, \dots, c_n \in \mathbb{F}$. An equation in the variables x_1, \dots, x_n is called **linear** if it can be expressed as $c_1x_1 + c_2x_2 + \dots + c_nx_n = b$.

Definition 10 – System of Equations

Let \mathbb{F} be a field, and $a_{ij} \in \mathbb{F}$ (where $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, n\}$). A **system of linear equations** in variables x_1, x_2, \dots, x_n is a finite collection of linear equations in x_1, x_2, \dots, x_n :

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m. \end{aligned}$$

A system of m equations with n unknowns is called an $m \times n$ **system**.

Definition 11 – Solutions

A **solution** to a linear equation $c_1x_1 + c_2x_2 + \dots + c_nx_n = b$ is a choice of field elements $s_1, s_2, \dots, s_n \in \mathbb{F}$, so that when we substitute them for x_1, x_2, \dots, x_n respectively, the resulting equation is true.

That is, we have $c_1s_1 + c_2s_2 + \dots + c_ns_n = b$ (i.e. the left- and right-hand sides are equal.)

A **solution to a system** is a choice of field elements s_1, s_2, \dots, s_n which solves *every* equation of the system.

Definition 12 – Consistent

If a system of equations has at least one solution, we say it is **consistent**.

If a system of equations has no solutions, we say it is **inconsistent**.

Definition 13 – Matrix

An $m \times n$ **matrix** over \mathbb{F} is a rectangular array of field elements consisting of m rows and n columns.

We denote the j^{th} entry in row i of matrix A , by a_{ij} , and call it the ij^{th} **entry** of A .

Definition 14 – Augmented Matrix

Consider a system of equations:

$$\begin{array}{ccccccc} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & b_2 \\ & \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & b_m \end{array}$$

We define the **augmented matrix** corresponding to the system of equations above to be:

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ & & \cdots & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array} \right),$$

Definition 15 – RREF

We say a matrix A is in **reduced row echelon form** if *all* of the following conditions are met:

- 1) All zero rows are at the bottom of the matrix A .
- 2) The first non-zero entry in each non-zero row is a 1. (Such entries are called “leading 1’s”.)
- 3) The leading 1’s move to the right, as we go down the rows of A .
- 4) All entries above and below a leading 1 are 0.

We will use the abbreviation “RREF” for “row-reduced echelon form”, for the rest of the text.

All matrices have a unique RREF.

Theorem 11 – Gaussian Elimination

To “row reduce” a matrix perform the following steps:

- 1) If the matrix consists entirely of 0’s, stop. It’s already row-reduced.
- 2) Find the first column with a non-zero entry and move the corresponding row to the top. (We will call the first non-zero entry a .)
- 3) Divide the row by the number a to obtain a leading one.
- 4) Subtract multiples of this row from the rows above and below, in order to make each entry above and below the leading 1 equal to 0.
- 5) Repeat 1-4 on the matrix consisting of the remaining rows.

Definition 16 – Variables

Suppose that R is a matrix in RREF. We say that x_i is a **leading variable** if column i contains a leading one. If a variable is not “leading” we call it a **non-leading variable**.

Remark 1. To solve a system:

- 1) Row reduce the augmented coefficient matrix.
- 2) If there is a row of the form $(\ 0 \ 0 \ \cdots \ 0 \ | \ 1 \)$ then there are no solutions.
- 3) Otherwise, assign the non-leading variables (if any) parameters, and use the equations coming from the rows of the RREF to solve for each variable in terms of the parameters.

△

Definition 17 – Homogeneous

A system of equations is called homogeneous if it is of the form

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= 0. \end{aligned}$$

In other words, it is homogeneous if the constant term (or right hand side) of *each* equation in the system is 0.

- $x_1 = 0, x_2 = 0, \dots, x_n = 0$ is *always* a solution to any homogeneous equation.
- We call this solution the *trivial* solution.
- Any other solution is called a *non-trivial* solution.

Chapter 3: Vector Spaces

Definition 18 – Vector Operators

Given two vectors \mathbf{v}, \mathbf{w} we define **their sum** $\mathbf{v} + \mathbf{w}$ using “tip to tail” addition (or the “parallelogram law of addition”). In the diagram in the margin, the vector $\mathbf{v} + \mathbf{w}$ is diagonal in the parallelogram spanned by \mathbf{v}, \mathbf{w} that shares its tail with \mathbf{v} and \mathbf{w} .

We can also define their **difference** $\mathbf{v} - \mathbf{w}$ geometrically using the same parallelogram: $\mathbf{v} - \mathbf{w}$ is the diagonal going from the tip of \mathbf{w} to the tip of \mathbf{v} .

Finally, given a vector \mathbf{v} and real number $a \in \mathbb{R}$, we can **scale \mathbf{v} by a** as follows:

- $0\mathbf{v} = \mathbf{0}$.
- If $a > 0$, then $a\mathbf{v}$ is a vector pointing in the same direction as \mathbf{v} with length scaled by a .
- If $a < 0$, then $a\mathbf{v}$ is a vector pointing in the opposite direction as \mathbf{v} with length scaled by $|a|$.

If $v = (x, y, z)$ and $w = (p, q, r)$, then $v + w = (x + p, y + q, z + r)$, $av = (ax, ay, az)$.

Definition 20 – \mathbb{F}^n

Let \mathbb{F} be a field. Consider the set $\mathbb{F}^n = \{(x_1, x_2, \dots, x_n) \mid x_1, x_2, \dots, x_n \in \mathbb{F}\}$. We can define two operations on \mathbb{F}^n which we call “vector addition” which is a map $\mathbb{F}^n \times \mathbb{F}^n \rightarrow \mathbb{F}^n$, and “scaling” which is a map $\mathbb{F} \times \mathbb{F}^n \rightarrow \mathbb{F}^n$ as follows.

For $v = (x_1, x_2, \dots, x_n), w = (y_1, y_2, \dots, y_n) \in \mathbb{F}^n$, and $c \in \mathbb{F}$ we define:

$$\begin{aligned} v + w &= (x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) && \text{(vector addition)} \\ &= (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n) \\ cv &= c(x_1, x_2, \dots, x_n) && \text{(scaling)} \\ &= (cx_1, cx_2, \dots, cx_n) \end{aligned}$$

Theorem 13 – \mathbb{F}^n

Let \mathbb{F} be a field. Set $\mathbf{0} = (0, 0, \dots, 0)$. For any $v, w, u \in \mathbb{F}^n$ and $a, b \in \mathbb{F}$ we have:

- 1) $v + w = w + v$.
- 2) $v + (w + u) = (v + w) + u$.
- 3) $a(v + w) = av + aw$.
- 4) $(a + b)v = av + bv$.
- 5) $(ab)v = a(bv)$.
- 6) $1v = v$.
- 7) $0 + v = v$.
- 8) For every $v \in V$ there exists $w \in V$ so that $v + w = \mathbf{0}$.

Definition 21 – Vector Space

Let \mathbb{F} be a field. A vector space V over \mathbb{F} is a non-empty set, containing a special element 0 , with two operations $V \times V \rightarrow V$ (called vector addition) and $\mathbb{F} \times V \rightarrow V$ (called scaling) so that for all $v, w, u \in V$ and $a, b \in \mathbb{F}$:

- 1) $v + w = w + v$.
- 2) $v + (w + u) = (v + w) + u$.
- 3) $a(v + w) = av + aw$.
- 4) $(a + b)v = av + bv$.
- 5) $(ab)v = a(bv)$.
- 6) $1v = v$.
- 7) $0 + v = v$.
- 8) For every $v \in V$ there exists $w \in V$ so that $v + w = 0$.

$P(\mathbb{F})$, $P_n(\mathbb{F})$ and \mathbb{F}^n are vector spaces.

Definition 22 – Matrix Cont.

Let \mathbb{F} be a field. An $m \times n$ **matrix** M **with entries in** \mathbb{F} is a rectangular array of elements of \mathbb{F} consisting of m rows and n columns.

We denote the entry in the i row and j column of a matrix m by m_{ij} .

The set of all $m \times n$ matrices with coefficients in \mathbb{F} is denoted by $\mathcal{M}_{m \times n}(\mathbb{F})$.

For example, a 2×3 matrix looks like $\begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \end{pmatrix} \in \mathcal{M}_{2 \times 3}(\mathbb{F})$, while a 3×2 matrix N

looks like $\begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \\ n_{31} & n_{32} \end{pmatrix} \in \mathcal{M}_{3 \times 2}(\mathbb{F})$.

$\mathcal{M}_{m \times n}(\mathbb{F})$, with pointwise addition and scaling is a vector space over \mathbb{F} ;

Corollary 2 – Vector Space

Let \mathbb{F} be a field, and V a vector space over \mathbb{F} . Then for any $v, w, u \in V$ and $a \in \mathbb{F}$ we have:

- 1) If $v + w = v + u$, then $w = u$.
- 2) If $a \neq 0$ and $av = aw$, then $v = w$.
- 3) The element $0 \in V$ is unique.
- 4) Additive inverses in V are unique. (This means that for each $v \in V$ there is only one element $w \in V$ which satisfies the condition of Axiom 8.)
- 5) $(-a)v = -(av)$. In particular $(-1)v = -v$.
- 6) $0v = 0$.
- 7) $a0 = 0$.

Definition 23 – Subspace

Let \mathbb{F} be a field and V a vector space over \mathbb{F} . We say that a subset $W \subseteq V$ is a **subspace of V** if W is also a vector space over \mathbb{F} using the same operations defined in V .

$P_n(\mathbb{F})$ is a subspace of $P(\mathbb{F})$.

$P_n(\mathbb{F})$ is a subspace of $P_m(\mathbb{F})$ if $n < m \in \mathbb{N}$.

Theorem 19 – Subspace

Let V be a vector space over a field \mathbb{F} . A **non-empty** subset $W \subseteq V$ is a subspace of V if and only if

- 1) For all $v, w \in W$ we have $v + w \in W$.
- 2) For all $v \in W$ and $c \in \mathbb{F}$ we have $cv \in W$.

Definition 24 – Trivial / Non-Trivial Subspace

Let V be a vector space over a field \mathbb{F} . The subspaces $\{0\}$ and V are called the **trivial subspaces** of V . Any other subspace W of V is called a **non-trivial subspace of V** .

In particular, we say that a subspace W is a non-trivial subspace of V if $W \neq \{0\}$ and $W \neq V$.

Chapter 4: Bases and Dimension

Definition 25 – Linear Combinatoin of Vectors

Let V be a vector space over \mathbb{F} , and $v_1, v_2, \dots, v_k \in V$. A vector of the form $a_1v_1 + a_2v_2 + \dots + a_kv_k \in V$ is called a linear combination of the vectors v_1, v_2, \dots, v_k .

Definition 26 – Span

Let V be a vector space over \mathbb{F} and $S \subseteq V$. We define the **span of S** , denoted $\text{span } S$, as follows:

- 1) If $S = \emptyset$ is empty, then $\text{span } S = \{0\}$.
- 2) Otherwise, $\text{span } S = \{a_1v_1 + a_2v_2 + \dots + a_kv_k \mid a_i \in \mathbb{F}, v_i \in S\}$ is the set of all possible linear combinations of vectors from S .

Theorem 20 – Span as Subspace

Let V be a vector space over \mathbb{F} and $S \subseteq V$ be **any** subset of vectors. Then the subset $\text{span } S \subseteq V$ is a subspace of V .

Definition 27 – S spans V

Let V be a vector space over \mathbb{F} . We say that a subset $S \subseteq V$ is a **spanning set for V** (or " S spans V ") if $V = \text{span } S$.

Definition 28 – Linearly Independnet

Let V be a vector space over \mathbb{F} . We say that a set S is **linearly independent** if for any vectors $v_1, v_2, \dots, v_k \in S$:

$$c_1v_1 + c_2v_2 + \dots + c_kv_k = 0 \implies c_1 = 0, c_2 = 0, \dots, c_k = 0.$$

Otherwise, we say that S is **linearly dependent**.

Definition 29 – Basis

Let V be a vector space over \mathbb{F} . A subset $\beta \subseteq V$ is called a **basis** if:

- 1) β spans V
- 2) β is linearly independent.

Vector space over \mathbb{F} also has basis.

Finite spanning set for V also contains basis for V .

Let \mathbb{F} be a field.

- 1) The set $\{e_1, e_2, \dots, e_n\}$ is a basis for \mathbb{F}^n .
- 2) The set $\{E_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for $\mathcal{M}_{m \times n}(\mathbb{F})$.
- 3) The set $\{1, x, x^2, x^3, \dots\}$ is a basis for $P(\mathbb{F})$.
- 4) The set $\{1, x, x^2, x^3, \dots, x^n\}$ is a basis for $P_n(\mathbb{F})$.



Theorem 23 – Unique Expression from Basis

Let V be a vector space over \mathbb{F} and β a basis of V . Then any $\mathbf{v} \in V$ has a unique expression

$$\mathbf{v} = \sum_{i=1}^n a_i \mathbf{v}_i$$

where $\mathbf{v}_i \in \beta$ and $a_i \in \mathbb{F}$.

Theorem 24 – The Replacement Theorem

Suppose that $\beta = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ is a basis for V and $I = \{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_k\}$ an independent subset of V . Then for any $i \in \{1, \dots, k\}$, we can obtain a new basis by replacing i elements of β with $\{\mathbf{w}_1, \dots, \mathbf{w}_i\}$. So after relabelling the elements* $\mathbf{v}_j \in \beta$ we have that the set $\beta_i = \{\mathbf{w}_1, \dots, \mathbf{w}_i, \mathbf{v}_{i+1}, \dots, \mathbf{v}_n\}$ is a basis for V .

Corollary 3

Suppose that V is a vector space over \mathbb{F} with a finite basis. Suppose that β is any basis of V and I is any independent set. Then $|I| \leq |\beta|$.

Theorem 25 – Size of Bases

Let V be a vector space over a field \mathbb{F} . If V has a finite basis, then all bases of V have the same size.

Definition 30 – Dimension

Let V be a vector space over \mathbb{F} with a finite basis. We define the **dimension of V** to be the size of a basis for V .

In this case, we say that V is **finite dimensional**. Otherwise, we say that V is infinite dimensional.

- 1) $\dim \mathbb{F}^n = n$.
- 2) $\dim \mathcal{M}_{m \times n}(\mathbb{F}) = mn$.
- 3) $\dim P_n(\mathbb{F}) = n + 1$.
- 4) $P(\mathbb{F})$ is infinite dimensional.

Corollary 4

Let V be a finite dimensional vector space over \mathbb{F} . S any spanning set for V , I any independent set in V , and β any basis. Then

$$|I| \leq |\beta| \leq |S|.$$

Chapter 5: Linear Transformations

Definition 31 – Linear Transformation

Let V and W be vector spaces over \mathbb{F} . A map $T : V \rightarrow W$ is called a **linear transformation** if:

$$\begin{aligned} T(v + w) &= T(v) + T(w) && \text{for all } v, w \in V \\ T(cv) &= cT(v) && \text{for all } v \in V \text{ and } c \in \mathbb{F} \end{aligned}$$

$T(x, y, z) = (2x - 4y + z, 3x - y + 2x)$ is a linear transformation from \mathbb{R}^3 to \mathbb{R}^2 .
 $T(p) = \frac{d}{dx}p$ is a linear transformation.

Theorem 26 – Properties of Linearity

Let V, W be vector spaces over \mathbb{F} .

- 1) If $T : V \rightarrow W$ is linear, then $T(0_v) = 0_w$.
- 2) The map $O : V \rightarrow W$ given by $O(v) = 0_w$ for all $v \in V$ is linear. This map is called the "zero map."
- 3) The map $I_V : V \rightarrow V$ given by $I_V(v) = v$ for all $v \in V$ is linear. This map is called the "identity map."

Theorem 27

Let V be a finite dimensional vector space over \mathbb{F} and $\beta = \{v_1, v_2, \dots, v_n\}$ a basis of V . A linear map $T : V \rightarrow W$ is uniquely determined by the values $T(v_1), T(v_2), \dots, T(v_n) \in W$.

Corollary 5 – Extending by Linearity

Let V, W be vector spaces over \mathbb{F} , and $\beta = \{v_1, \dots, v_n\}$ a basis for V . Given a list of (not necessarily distinct) vectors $w_1, \dots, w_n \in W$ there is exactly one linear map $T : V \rightarrow W$ so that $T(v_i) = w_i$.

This map is defined for all $v \in V$ as follows. Writing $v = \sum_{i=1}^n a_i v_i$, we then set $T(v) = \sum_{i=1}^n a_i w_i$.

This process is called "extending by linearity".

Theorem 28 – Composition of Linear Maps

Let V, W, X be vector spaces over \mathbb{F} . If $T : V \rightarrow W$ and $S : W \rightarrow X$ are linear maps, then the composition $S \circ T : V \rightarrow X$ is linear.

Theorem 29 – Null Space / Image

Let V, W be vector spaces over \mathbb{F} and $T : V \rightarrow W$ a linear transformation. The sets:

$$N(T) = \{v \in V \mid T(v) = 0\} \subseteq V$$

$$\text{im}(T) = \{w \in W \mid w = T(v) \text{ for some } v \in V\} \subseteq W$$

are subspaces of V, W respectively.

The subspace $N(T)$ is called the **null space** of T .

The subspace $\text{im}(T)$ is called the **image** of T .

Definition 32 – rank

Let V, W be vector spaces over \mathbb{F} and $T : V \rightarrow W$ linear. We define the **rank** of T by $\text{rank } T = \dim \text{im}(T)$.

Theorem 30 – The Dimension Theorem

Let V, W be finite dimensional vector spaces over \mathbb{F} . If $T : V \rightarrow W$ linear, then

$$\dim V = \dim N(T) + \dim \text{im}(T)$$

.

Chapter 6: Matrix Algebra (Appendix A)

Definition 33 – Matrix Multiplication

Let $A \in \mathcal{M}_{m \times n}(\mathbb{F})$ and $B \in \mathcal{M}_{n \times k}(\mathbb{F})$. We define their product $AB \in \mathcal{M}_{m \times k}(\mathbb{F})$ as follows: for $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, k\}$ the ij -entry of the product AB is given by

$$(AB)_{ij} = \sum_{l=1}^n A_{il}B_{lj}.$$

$$AB \neq BA.$$

Definition 34 – Special Matrices

For each $n, m \in \mathbb{N}$ we define the following matrices:

- 1) $O_{m,n} \in \mathcal{M}_{m \times n}(\mathbb{F})$ - the matrix consisting of all 0's. In other words $(O_{m,n})_{i,j} = 0$ for all $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, n\}$.
- 2) $I_n \in \mathcal{M}_{n \times n}(\mathbb{F})$ - the matrix with 1's on the diagonals, and 0 in all other entries. In other words

$$(I_n)_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

$$O_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$



Theorem 31

Let \mathbb{F} be a field, $A, A_1, A_2 \in \mathcal{M}_{m \times n}(\mathbb{F})$, $B, B_1, B_2 \in \mathcal{M}_{n \times k}(\mathbb{F})$, $C \in \mathcal{M}_{k \times p}(\mathbb{F})$ and $c \in \mathbb{F}$.

1. $A(BC) = (AB)C$
2. $(A_1 + A_2)B = A_1B + A_2B$
3. $A(B_1 + B_2) = AB_1 + AB_2$
4. $I_m A = A = A I_n$
5. $O_{rm} A = O_{rn}$ for any $r \in \mathbb{N}$.
6. $A(cB) = c(AB) = (cI_m)AB = AB(cI_k) = A(cI_n)B$.

Definition 35 – Invertibility

Let $A \in \mathcal{M}_{n \times n}(\mathbb{F})$. We say that A is **invertible** if there exists a matrix $B \in \mathcal{M}_{n \times n}(\mathbb{F})$ so that $AB = I_n = BA$.

Theorem 32

Let $A, B \in \mathcal{M}_{n \times n}(\mathbb{F})$.

- 1) If A is invertible, then the inverse of A is unique.
- 2) If A is invertible, then A^{-1} is also invertible.
- 3) If A and B are invertible, then AB is invertible.
- 4) I_n is invertible.
- 5) If $AB = I_n$, then A is invertible and $B = A^{-1}$.

Definition 36 – A^t

Let $A \in \mathcal{M}_{m \times n}(\mathbb{F})$. We define the matrix $A^t \in \mathcal{M}_{n \times m}(\mathbb{F})$ by:

$$(A^t)_{ij} = A_{ji}.$$

In other words, to obtain A^t we "swap the rows and columns of A ."

Definition 37 – Symmetric

We say that $A \in \mathcal{M}_{n \times n}(\mathbb{F})$ is **symmetric** if $A^t = A$. We denote the set of all symmetric matrices by $\mathbf{Sym}_n(\mathbb{F})$.

We say that $A \in \mathcal{M}_{n \times n}(\mathbb{F})$ is **skew-symmetric** if $A^t = -A$. We denote the set of all skew-symmetric matrices by $\mathbf{Sk}_n(\mathbb{F})$.

Theorem 33

Let $A, B \in \mathcal{M}_{m \times n}(\mathbb{F})$, $C \in \mathcal{M}_{n \times k}(\mathbb{F})$ and $c \in \mathbb{F}$.

1. $(A + B)^t = A^t + B^t$
2. $(cA)^t = cA^t$
3. $(A^t)^t = A$
4. $(AC)^t = C^t A^t$.
5. In the case that $m = n$, we also have that if $A \in \mathcal{M}_{n \times n}(\mathbb{F})$ is invertible, then $A^t \in \mathcal{M}_{n \times n}(\mathbb{F})$ is invertible and $(A^t)^{-1} = (A^{-1})^t$.

Definition 38 – Diagonal and Triangular

We say that A is **diagonal** if $A_{ij} = 0$ for all $i \neq j$.

Let $A \in \mathcal{M}_{n \times n}(\mathbb{F})$. We say that A is **upper triangular** if $A_{ij} = 0$ for all $i > j$. This means that all entries below the diagonal of A must be 0.

Similarly, we say that A is **lower triangular** if $A_{ij} = 0$ for all $i < j$. This means that all entries above the diagonal of A must be 0.

We say that A is **strictly upper-triangular** if $A_{ij} = 0$ for all $i \geq j$.