MATH 554: Linear Algebra Qualifying Exam Prep

Kale Stahl

Contents

I Notes **1**

1 Preliminary Definitions **1**
Definition: Group . . . 1
Definition: Ring . . . 1
Definition: Field . . . 1
Definition: Vector Space . . . 1
Definition: Left Module . . . 2
Definition: Ideal . . . 2
Definition: Subring . . . 2
Definition: Monoid . . . 2
Definition: Ring Homomorphism . . . 3
Definition: Isomorphism . . . 3
Theorem: First Isomorphism Theorem . . . 4

2 Domains and Fields of Fractions **5**
Definition: Maximal Ideal . . . 5
Definition: Integral Domain . . . 5
Definition: Field of Fractions . . . 5
Proposition: Universal Mapping Property . . . 6
Definition: Euclidean Domain . . . 7
Definition: Principle Ideal Domain . . . 7
Definition: Ideal Addition . . . 8
Definition: Ideal Multiplication . . . 8
Theorem: Chinese Remainder Theorem . . . 9

3 Modules and Tensor Products **10**
Definition: Addition of Submodules . . . 10
Definition: Span of a Module . . . 10
Definition: External Direct Sum . . . 10
Definition: Internal Direct Sum . . . 10
Definition: Free Modules . . . 10
Theorem: Universal Mapping Property for Free Modules . . . 11
3.1 Tensor Products . . . 11
Definition: Tensor Product . . . 11
Definition: Balanced Map . . . 12
Theorem: Universal Mapping Property for Balanced Maps . . . 12
Theorem: Universal Mapping Property for Quotients . . . 12
Definition: Bimodule . . . 12
3.2 Algebra Structures . . . 13

4 Linear and Multi-Linear Algebra **15**
Corollary: Rank-Nullity Theorem . . . 15
Definition: Dual Space . . . 15
Definition: Adjoint Map . . . 16
Definition: Symmetric Group . . . 16
Definition: Sign Function . . . 17
Theorem: Expansion by Minors . . . 18

4.1 An Excursion into Multivariate Calculus . . . 19
Definition: Cross Product . . . 20

5 Matrix Algebra **21**
Definition: Jordan Block . . . 22
Definition: Generalized Eigenvector . . . 22

6 Spectral Theory **23**
Definition: Inner Product . . . 23
Theorem: Spectral Theorem . . . 23

Part I
Notes

These notes are based on the MA 554: Linear Algebra class taught by Dr. Jeremy Miller in Fall 2025 at Purdue. The first half of the notes are based on [1], and the rest are based on various books with most coming from [2]. They are meant to prepare for the qualifying exam in Linear algebra. Unless specified otherwise, suppose R is a ring, I, J are ideals, and M is a module.

1 Preliminary Definitions

Definition 1.1: Group.
A group is a set G and maps $G \times G \to G$ such that

(a) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *for all* $a, b, c \in G$.

(b) *There exists an element e with $a = ae = ea$ for all $a \in G$.*

(c) *For any $a \in G$, there exists an element $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.*

A group is considered abelian if it is also commutative. Groups are sets with a single operation, but we can extend this to two operations by considering rings.

Definition 1.2: Ring.
A ring R is a set with two operations, $+, \times : R \times R \to R$ with

(a) $(R, +)$ *is an abelian group with* $e = 0$.

(b) $a \times (b \times c) = (a \times b) \times c$ *for all* $a, b, c \in R$.

(c) *There exists $1 \in R$ with $1 \times a = a \times 1 = a$ for all a.*

(d) $(a + b) \times c = a \times c + b \times c$ *and* $c \times (a + b) = c \times a + c \times b$ *for all* $a, b, c \in R$.

Rings are considered commutative if their $\times$ operation is commutative. We can further define sets with multiple operations by considering Fields.

Definition 1.3: Field.
A field is a set F and two operations $+, \cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ such that

(a) $a + (b + c) = (a + b) + c$ *for all* $a, b, c \in \mathbb{F}$

(b) $a + b = b + a$ *for all* $a, b \in \mathbb{F}$

(c) *There exists $0, 1 \in \mathbb{F}$ with $0 + a = a$ and $1 \cdot a = a$ for all $a \in \mathbb{F}$.*

(d) $a(b + c) = ab + ac$ *and* $(a + b)c = ac + bc$ *for all* $a, b, c \in \mathbb{F}$.

(e) $ab = ba$ *for all* $a, b \in \mathbb{F}$.

(f) *For all $a \neq 0$, there exists an a^{-1} such that $aa^{-1} = a^{-1}a = 1$.*

Definition 1.4: Vector Space.
Let $\mathbb{F}$ ne a field. An $\mathbb{F}$-vector space is a set V and two operations $+ : V \times V \to V$ and $\cdot : \mathbb{F} \times V \to V$ such that

(a) $(\vec{a} + \vec{b}) + \vec{c} = \vec{a} + (\vec{b} + \vec{c})$ *for all* $\vec{a}, \vec{b}, \vec{c} \in V$.

(b) *There exists a $\vec{0} \in V$ with $\vec{0} + \vec{a} = \vec{a}$.*

(c) *For all $\vec{a} \in V$, there exists $-\vec{a} \in V$ with $\vec{a} + (-\vec{a}) = \vec{0}$.*

(d) $r(\vec{a} + \vec{b}) = r\vec{a} + r\vec{b}$ *for all* $\vec{a}, \vec{b} \in V$ *and* $r \in \mathbb{F}$.

(e) $(r + s)\vec{a} = r\vec{a} + s\vec{a}$ *for all* $r, s \in \mathbb{F}$ *and* $\vec{a} \in V$.

Note that a ring as in Definition 1.2 is a set satisfying all axioms of a field in Definition 1.3 except for **(e)** and **(f)**. If it is a commutative ring, then it satisfies **(e)**.

Example 1.1

$\mathbb{Z}$ is a commutative ring, but not a field.

Definition 1.5: Left Module.
Let R be a ring. A left R-module is a set with two operations satisfying the conditions of Definition 1.4

Definition 1.6: Ideal.
Let R be a commutative ring. A set $I \subseteq R$ is an ideal if

- ***(a)*** $0 \in I$.
- ***(b)*** *For all $a, r \in I$,we have $ar \in I$.*
- ***(c)*** *For all $a, b \in I$, then $a + b \in I$.*

Definition 1.7: Subring.
Let R be a ring. A set $K \subseteq R$ is an subring if

- ***(a)*** $0, 1 \in K$.
- ***(b)*** *For all $a, r \in K$, we have $ar \in K$.*
- ***(c)*** *For all $a, b \in K$, we have $a + b \in K$.*

Proposition 1.8.
A commutative ring R is a field if and only if $\{0\}, R$ are the only ideals.

Definition 1.9.
Let R be a ring. Then define

$$R[x] = \left\{r_1 + r_1 x + r_2 x^2 + \cdots + r_n x^n : r_0, \ldots, r_n \in R\right\} \tag{1.1}$$

Proposition 1.10.
If R is commutative, then so is $R[x]$.

Theorem 1.11.
If $\mathbb{F}$ is a field, all ideals in $\mathbb{F}[x]$ are of the form $(f(x)), f(x) \in \mathbb{F}[x]$.

Lemma 1.12.
Let $f(x), g(x) \in \mathbb{F}[x]$. Then there exist some $d(x), r(x)$ with $\deg r(x) < \deg f(x)$ such that

$$g(x) = d(x)f(x) + r(x) \tag{1.2}$$

Definition 1.13.
Let V, W be $\mathbb{F}$-vector spaces. Then $f : V \to W$ is linear if

- ***(a)*** $f(\vec{x} + \vec{y}) = f(\vec{x}) + f(\vec{y})$ *for all* $\vec{x}, \vec{y} \in V$.
- ***(b)*** $f(r\vec{x}) = rf(\vec{x})$ *for all* $\vec{x} \in V$ *and* $r \in \mathbb{F}$.

Proposition 1.14.
The data of an $\mathbb{F}[x]$-module is a vector space V and a linear map $f : V \to V$.

Definition 1.15: Monoid.
A monoid is a set M and a map $\cdot : M \times M \to M$ such that

- ***(a)*** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all* $a, b, c \in M$.
- ***(b)*** *There exists a $1 \in M$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in M$.*

Note that a monoid is a group as seen in Definition 1.1, except it does not necessarily include inverses.

Example 1.2

$(\mathbb{N}, +)$ is a monoid, but not a group. It clearly has associativity and the identity since $1 \in \mathbb{N}$, but there are no inverses since we would need -1, but $1 \notin \mathbb{N}$ so it is a monoid but not a group.

Definition 1.16.
Let R be a ring, and M a monoid. Define

$$R[M] = \{r_1 m_1 + r_2 m_2 + \cdots + r_n m_n : r_i \in R, m_i \in M\} \tag{1.3}$$

Definition 1.17.
Let M, N be monoids. $f : M \to N$ is a map with

$$f(m_1 m_2) = f(m_1) f(m_2) \tag{1.4}$$

for all $m_1, m_2 \in M$.

Proposition 1.18.
Let V be an R-module. A $R[M]$-module structino on V is a monoid homomorphism $M \to \hom_R(V, V)$. If M is a group, then $M \to \mathrm{Aut}_R(V, V)$.

Proposition 1.19.
$\hom_R(V, V)$ *is a ring with $f : V \to V$ and $g : V \to V$ such that*

$$(f + g)(v) = f(v) + g(v) \tag{1.5}$$

for all $v \in V$.

Definition 1.20: Ring Homomorphism.
Let R, R' be rings. A function $f : R \to R'$ is a ring homomorphism if

(a) $f(r_1 r_2) = f(r_1) f(r_2)$ *for all $r_1, r_2 \in R$.*

(b) $f(r_1 + r_2) = f(r_1) + f(r_2)$ *for all $r_1, r_2 \in R$.*

Definition 1.21: Isomorphism.
A homomorphism $f : R \to R'$ is an isomorphism if there is an inverse homomorphism $f^{-1} : R' \to R$ such that

$$f^{-1} \circ f(x) = x \tag{1.6}$$

for all $x \in R$. If it exists, we say $R \cong R'$.

Theorem 1.22.
let $\mathbb{F}$ be a field. Then $\mathrm{Mat}_{\mathbb{F}}(n, n) \cong \hom_{\mathbb{F}}(\mathbb{F}^n, \mathbb{F}^n)$.

Definition 1.23.
Let $f : R \to R'$ be a ring homomorphism. Then define the kernel of f as

$$\ker(f) = \{r \in R : f(r) = 0\} \tag{1.7}$$

Proposition 1.24.
$\ker(f) \subseteq R$ *is an ideal.*

Definition 1.25.
Let $f : R \to R'$ be a ring homomorphism. Then

$$\mathrm{im}(f) = \{x | f(r) = x, \forall r \in R\} \tag{1.8}$$

Proposition 1.26.
$\mathrm{im}(f) \subseteq R'$ *is a subring.*

Theorem 1.27: First Isomorphism Theorem.
Let $f : R \to S$ be a ring homorphism. Then

$$R/\ker(f) \cong \mathrm{im}(f) \tag{1.9}$$

Proposition 1.28.
If R is a ring, then there exists a unique $f : \mathbb{Z} \to R$ which is a ring homomorphism.

Definition 1.29.
Let A be an abelian group and $B \subseteq A$ a subgroup. Define the equivalence class of $a \in A$ be

$$[a] = \{a + b : b \in B\} \tag{1.10}$$

We define a quotient group by

$$A/B = \{[a] : a \in A\} \tag{1.11}$$

Proposition 1.30.
Let $I \subseteq R$ be an ideal. Then the map $f : R \to R/I$ is surjective.

Proposition 1.31.
Let $K \subseteq R$ be a subring. Then the map $g : K \to R$ is injective.

2 Domains and Fields of Fractions

Definition 2.1: Maximal Ideal.
$I \subset R$ is called a maximal ideal if

1. *$I \neq R$*
2. *$J \subseteq I$ implies that either $J = R$ or $J = I$.*

Proposition 2.2.
Let $\mathbb{F}$ be a field. $\mathbb{F}$ and $\{0\}$ are the only ideals of $\mathbb{F}$.

Corollary 2.3.
0 is a maximal ideal in $\mathbb{F}$.

Definition 2.4: Integral Domain.
R is an integral domain if

(a) *R is commutative*

(b) *If $ab = 0$ then $a = 0$ or $b = 0$.*

Corollary 2.5.
If R is commutative and $M \subsetneq R$ is maximal, then M is prime.

Definition 2.6: Field of Fractions.
Let R be a commutative ring and $S \subseteq R$ a multiplicatively closed subset. Assume $1 \in S$. Let $S^{-1}R = (R \times S)/\sim$ defining an equivalence relation by saying

$$\frac{r}{s} \sim \frac{r'}{s'} \tag{2.1}$$

if there exists a nonzero t such that $trs' = tr's$. This t can be ignored if R is an integral domain.

Example 2.1

If $S = \{0, 1\}$ then $S^{-1}R = 0$ and $\frac{r}{s} = \frac{0}{0}$.

Example 2.2

If $R = \mathbb{Z}$ and $S = \mathbb{Z} - \{0\}$ then $S^{-1}R = \mathbb{Q}$.

Definition 2.7.
Define $\mathbb{F}(x) = S^{-1}\mathbb{F}[x] = \left\{ \frac{f(x)}{g(x)} : g(x) \neq 0 \right\}$ with $S = \mathbb{F}[x] - \{0\}$.

Theorem 2.8.
If $f(x) \in \mathbb{F}[x, x^{-1}]$ has an inverse, then $f(x) = ax^k$ for $a \neq 0$ and $k \in \mathbb{Z}$.

Corollary 2.9.
$\frac{1}{x+1} \notin \mathbb{F}[x, x^{-1}]$

Definition 2.10.
For $s \in \{1, a, a^2, \dots\} \subset R$, write $s^{-1}R = R[a^{-1}]$.

Example 2.3

$\mathbb{Z}[2^{-1}] = \left\{ \frac{x}{2^n} \right\} \subseteq \mathbb{Q}$

Example 2.4

$\mathbb{Z}[2^{-1}][3^{-1}] \cong \mathbb{Z}[6^{-1}]$

Proposition 2.11.
$S^{-1}R$ is a ring.

Definition 2.12.
Let $\iota : R \to S^{-1}R$ be $\iota(t) = \frac{t}{1}$.

Proposition 2.13.
$\iota : R \to S^{-1}R$ is a ring homomorphism.

Proposition 2.14.
If R is an integral domain, then ι is injective.

Proof. Suppose $\iota(r) = 0$. Then $\frac{r}{1} = \frac{0}{1}$ meaning that $t \cdot r \cdot 1 = t \cdot 1 \cdot 0$ for some $t \neq 0$. This implies that $r = 0$ or $t = 0$, but since t cannot be zero, so ι must be injective. $\square$

Proposition 2.15: Universal Mapping Property.
Suppose $S \subset R$ and let $f : R \to R'$ be a ring homomorphism. Suppose for all $x \in S$, $f(x)$ has an inverse. Then there exists a unique $g : S^{-1}R \to R'$ with $g \circ \iota = f$.

Definition 2.16.
If R is an integral domain, let $\mathrm{Frac}(R) = S^{-1}R$ with $S = R - \{0\}$.

Example 2.5

$\mathrm{Frac}(\mathbb{F}[x]) = \mathbb{F}[x]$

Example 2.6

$\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$

Proposition 2.17.
$\mathrm{Frac}(R)$ is a field. Proposition 2.15 shows that this is the smallest field that you can embed your ring into.

Corollary 2.18.
If R is an integral domain, $\mathbb{F}$ is a field, and $f : R \to \mathbb{F}$ is injective, then there exists a function $g : \mathrm{Frac}(R) \to \mathbb{F}$ injective with

$$\begin{tikzcd}
R \arrow[r, hook, "f"] \arrow[d, hook, "\iota"] & \mathbb{F} \\
\mathrm{Frac}(R) \arrow[ur, hook, "g"] &
\end{tikzcd}$$

Figure 1

Proposition 2.19.
Let $\mathbb{F}, \mathbb{K}$ be fields and $g : \mathbb{F} \to \mathbb{K}$ be a homomorphism. Then g is injective.

Proof. Suppose $g(a) = 0$. Then

$$1_{\mathbb{K}} = g(1_{\mathbb{F}}) = g(aa^{-1}) = 0g(a^{-1}) = 0 \tag{2.2}$$

which is a contradiction, so $a = 0$ and g is injective. $\square$

Definition 2.20.
If M is an R-module, $1 \in S \subseteq R$, S is closed under multiplication, and R is commutative, then let

$$S^{-1}M = M \times S / \sim \tag{2.3}$$

with $\frac{m}{s} \sim \frac{m'}{s'}$ if $tms' = tm's$ for $t \neq 0$.

Proposition 2.21.
$S^{-1}M$ is a $S^{-1}R$-module.

Definition 2.22: Euclidean Domain.
Let R be an integral domain. We call R Euclidean if there is $N : R \to \mathbb{N}$ such that for all $r \in R$

(a) *$N(r) = 0$ if and only if $r = 0$*

(b) *for all $a, b \in R$ with $b \neq 0$ there exists some d, r with $a = db + r$ and $N(r) < N(a)$.*

Theorem 2.23.
If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is Euclidean with $N = \deg +1$.

Theorem 2.24.
If $\mathbb{F}$ is a field, then $\mathbb{F}$ is Euclidean.

Definition 2.25: Principle Ideal Domain.
Let R be an integral domain. R is a PID if all ideals are of the form (r) for $r \in R$.

Theorem 2.26.
If R is Euclidean, then R is a PID.

Proof. Let $I \subset R$ be an ideal. Assume $I \neq 0$. LEt $D = \min_{i \in I, i \neq 0} N(i) \in \mathbb{N}_0$ and $D > 0$. Pick B with $N(b = D$. Consider $a \in I$. We want to show that $a \in (b)$, so then $I = (b)$. We can write $a = db + r$ with $N(r) < N(b)$ for some $r \in I$, so then

$$0 = N(t) < N(b) = D \tag{2.4}$$

Which implies that $r = 0$ so $a = db$ meaning $a \in (b)$. □

Corollary 2.27.
$\mathbb{Z}[x]$ is not Euclidean.

Definition 2.28.
u is a unit if there exists some w such that

$$uw = wu = 1 \tag{2.5}$$

Definition 2.29.
Let R be commutative, and $a, b \in R$ with $b \neq 0$. We write $a|b$ if there exists some $c \in R$ with $ac = b$.

Definition 2.30.
Let R be a commutative ring. We say that x is the gcd *of $a, b \in R$ if*

(a) *$x|a$*

(b) *$x|b$*

(c) *for all y, $y|a$ and $y|b$ implies $y|x$*

Definition 2.31.
For $a_1, \ldots, a_k \in R$, let

$$(a_1, \ldots, a_k) = \{r_1 a_1 + \ldots r_k a_k : r_i \in R\} \tag{2.6}$$

Proposition 2.32.
If $(a, b) = (x)$ then $x = \gcd(a, b)$.

Proof. First, assume $y|a$ and $y|b$. We want to show that $y|x$. We know that $a \in (y)$ and $b \in (y)$ so $x = (a, b) \subset (y)$. So then $x \in (y)$ so $y|x$. □

Proposition 2.33.
If R is an integral domain and $(d) = (d')$, then $d' = du$ for a unit u.

Proof. Assume $d, d' \neq 0$. we have that $d \in (d) = (d')$ so $d = xd'$ and $d' = yd$ for some $x, y \in R$. So then

$$d = xyd \tag{2.7}$$
$$0 = (1 - xy)d \tag{2.8}$$

Since $d \neq 0$, $1 - xy = 0$ meaning that $xy = 1$ so x and y are units. □

Corollary 2.34.
If R is a PID, then gcd *exists and are unique up to a unit.*

In a Euclidean domain, it is of interest to directly compute $\gcd(a, b)$. To this end, we have a scheme:

1. Assume $N(a) \leq N(b)$ and $r_0 = b$ and $r_1 = a$.
2. Write $r_i = dr_{i+1} + r_{i+2}$ with $N(r_{i+2}) \leq N(r_{i+a})$.
3. Repeat until you find a k such that $r_k = 0$.
4. Then $r_{k-1} = gcd(a, b)$.

This is essentially applying the Euclidean Algorithm repeatedly until you find the smallest generator of the elements.

Definition 2.35: Ideal Addition.
For $I, J \subseteq R$ be ideals. Define

$$I + J = \{i + j : i, i \in I, J \in J\} \tag{2.9}$$

Proposition 2.36.
For I, J ideals, $I + J$ is also an ideal.

Proposition 2.37.
If R is a PID with ideals $(a), (b)$, then

$$(a) + (b) = (\gcd(a, b)) \tag{2.10}$$

Definition 2.38.
Let R, S be rings. $R \times S$ is a ring with

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \tag{2.11}$$
$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2) \tag{2.12}$$

Note that $R \times S$ will not necessarily be an integral domain if $1 \neq 0$ in R and S.

Definition 2.39.
I and J are comaximal if $I + J = R$.

Example 2.7

$(6) + (25) = \mathbb{Z}$, so $(6), (25)$ are comaximal ideals in $R = \mathbb{Z}$.

Definition 2.40: Ideal Multiplication.
Let R be a commutative ring and I, J ideals. Define

$$IJ = \left\{\sum i_n j_n : i_n \in I, j_n \in J\right\} \tag{2.13}$$

Proposition 2.41.
IJ is an ideal.

Proposition 2.42.
$IJ \subseteq I \cap J$

Proof. Let $x \in IJ$. We want to show that $x \in I$ and $x \in J$. We know that $x = \sum i_n j_n$, and we want to show that each term $i_n j_n$ in the sum is in both I and J. □

Theorem 2.43: Chinese Remainder Theorem.
Let $A_1, \dots, A_k \subseteq R$ be ideals. Let $: R \to R/A_1 \times \cdots \times R/A_k$ be defined as

$$f(r) = ([r], \dots, [r]) \tag{2.14}$$

If $A_i + A_j = R$ for all $i \neq j$, then

(a) $\ker(f) = \bigcap_{i=1}^k A_i$

(b) *f is surjective*

(c) $\bigcap_{i=1}^k A_i = A_1 A_2 \dots A_k$

Proof. **(a)** An element $r \in \ker(f)$ if and only if $f(r) = 0$ which can happen if and only if $([r], \dots, [r]) = ([0], \dots, [0])$ which is true if and only if $r \in A_1 \cap A_2 \cap \cdots \cap A_k$ which is what we want.

(b) For $k = 2$, assume $A + B = R$. We want to show that $f : R \to R/A \times R/B$ is surjective. Pick some $[r] \in R/A$ and $[s] \in R/B$. Then $A + B = R$ implies that there are some $a \in A$ and $b \in B$ with $a + b = 1$. So then we see

$$f(ra + sb) = ([ra + sb], [ra + sb]) \tag{2.15}$$

We need to check if this is in $[r]$, so we take $ra + sb - r$ and see

$$[ra + sb]_A = [sb] = [s(1 - a)] = [s - as] = [s] \in A \tag{2.16}$$

so we are finished. We can proceed by induction on k, which is left as an exercise.

(c) Again, assume $k = 2$ so we need to show that $A \cap B = AB$. Clearly $AB \subseteq A \cap B$, so we only need to show that $A \cap B \subseteq AB$. Pick some $c \in AB$. We then see

$$c = 1c = (a + b)c = ac + bc \in AB \tag{2.17}$$

which proves the $k = 2$ case. We can again induct on k to get the rest.

□

Example 2.8

Let $R = \mathbb{Z}$, $A_1 = (2)$, $A_2 = (3)$. Then $f : \mathbb{Z} \to \mathbb{Z}/2 \times \mathbb{Z}/3$ gives us

$$A_1 + A_2 = (2) + (3) = (1) = \mathbb{Z} \tag{2.18}$$
$$A_1 A_2 = (2)(3) = (6) \tag{2.19}$$

and

$$\ker(f) = A_1 A_2 = (6) \tag{2.20}$$
$$\operatorname{im}(f) = \mathbb{Z}/2 \times \mathbb{Z}/3 \tag{2.21}$$

So then by Theorem 1.27, we have that $\mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3$.

Example 2.9

$\mathbb{R}[x]/(x^2 + 1) = \mathbb{C}$

3 Modules and Tensor Products

We will now consider modules and their applications to linear algebra.

Definition 3.1: Addition of Submodules.
Let $A_1, \ldots A_k \subseteq M$ be submodule. Then we define

$$A_1 + \cdots + A_k = \{a_1 + \ldots a_k : a_i \in A_i\} \tag{3.1}$$

Proposition 3.2.
$A_1 + \cdots + A_k$ is a submodule.

Example 3.1

If $R = \mathbb{Z}$ and $M = \mathbb{Z}^2$ and

$$A = \left\{ \begin{bmatrix} x \\ 0 \end{bmatrix} : 2|x \right\} = \text{Span} \begin{bmatrix} 2 \\ 0 \end{bmatrix} \tag{3.2}$$

$$B = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} : x = y \right\} = \text{Span} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \tag{3.3}$$

Then $A + B \cong \mathbb{Z}^2$ and $M/A + B \cong \mathbb{Z}/2$.

Theorem 3.3.
Let M and N be R-modules and $A, B \subseteq M$ be submodules. Then

(a) *For $f : M \to N$ which is R linear, then $M/\ker f \cong \operatorname{im} f$.*

(b) $(A + B)/B \cong A/A \cap B$

(c) *If $A \subseteq B$, then $(M/B)/(B/A) \cong M/B$.*

(d) *$\{M \supseteq C \supseteq A\} \cong \{M/A \supseteq C' \supseteq 0\}$ for some C, C' submodules where $\pi : M \to M/A$ defines $C \mapsto C/A$ and $C' \mapsto \pi^{-1}(C')$.*

Definition 3.4: Span of a Module.
Let $S \subseteq M$ be a set and M an R-module. Then

$$\text{Span}_R(S) = \langle S \rangle_R = \left\{ \sum r_i s_i : r_i \in R, s_i \in S \right\} \tag{3.4}$$

We say that S generates M if $\langle S \rangle = M$. M is finitely generated if $M = \langle s_1, \ldots, s_n \rangle$ for some finite n. We say that M is cyclic if $M = \langle S \rangle$ for some S.

Definition 3.5: External Direct Sum.
Let M and N be R-Modules. Let $M \oplus N = M \times N$, and define

$$(n_1, n_1) + (m_2, n_2) = (n_1 + m_1, n_2 + m_2) \tag{3.5}$$
$$r(n_1, n_1) = (rn_1, rn_2) \tag{3.6}$$

Definition 3.6: Internal Direct Sum.
Let $A, B \subseteq M$ be submodules. We say that $M = A \oplus_{internal} B$ if there is some map $A \oplus B \to M$ such that $(a, b) \mapsto a + b$ is an isomorphism.

Definition 3.7: Free Modules.
For a set S, a ring R, we define the free R-module over S, $F_R(S)$ as

$$F_R(S) = \{f : s \to R | f(s) = 0 \textit{ for all but finitely many } s \in S\} \tag{3.7}$$

Definition 3.8.
There is a natural map $\iota : S \to F_R(S)$ such that for all $s \in S$ we have $\iota(s) : S \to R$. We can define

$$(\iota(s))(t) = \begin{cases} 1 & s = t \\ 0 & s \neq t \end{cases} \tag{3.8}$$

This acts as a sort of "indicator" function. Using this, we can establish a universal mapping property for free modules.

Theorem 3.9: Universal Mapping Property for Free Modules.
Let S be a set, M be an R-module and $f : S \to M$, then there exists a unique $\widehat{f} : F_R(S) \to M$ which is R-linear and makes Figure 2 commute.

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[d, hook, "\iota"'] & M \\ F_R(S) \arrow[ur, "\widehat{f}"'] & \end{tikzcd}$$

Figure 2

This process is analogous to how we can characterize a linear operator by its action on a basis, but now we are associating a set with a free module rather than a basis in the traditional since. We can now define a basis for an R-module.

Definition 3.10.
Let M be an R-module. We say that a set $S \subseteq M$ is a basis if for any map i we have that Figure 3 implies $F_R(S) \cong M$.

$$\begin{tikzcd} S \arrow[r, "i"] \arrow[d, hook, "\iota"'] & M \\ F_R(S) \arrow[ur, "\widehat{i}"'] & \end{tikzcd}$$

Figure 3

Example 3.2

If we let $R = \mathbb{R}$ and $M = \mathbb{R}^2$ we can let

$$S = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\}$$

We have that $F_{\mathbb{R}}(S) \to \mathbb{R}^2$ is an isomorphism, meaning S is a basis for $\mathbb{R}^2$, which is consistent to what we know from the theory of basis' in linear algebra.

3.1 Tensor Products

Definition 3.11: Tensor Product.
Let R be a ring, M a right R-module and N a left R-module. Then we define

$$M \otimes_R N = F_{\mathbb{Z}}(M \times N)/A \tag{3.9}$$

where

$$A = \langle (mr) \times n - m \times (rn),\ (m_1 + m_2) \times n - (m_1 \times n) - (m_2 \times n),\ m \times (n_1 + n_2) - m \times n_1 - m \times n_2 \rangle \tag{3.10}$$

for some $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $r \in R$. We write $m \otimes n$ for the image of $m \times n \in M \times n$ in $F_{\mathbb{Z}}(M \times N)$. We also write for $x \in M \otimes N$

$$x = \sum_i k_i (m_i \otimes n_i), \qquad k_i \in \mathbb{Z}, m_i \in M, n_i \in N \tag{3.11}$$

Finally, we have the following rules for all elements $m \in M$, $n \in N$ and $r \in R$:

$$(mr) \otimes n = m \times (rn) \tag{3.12}$$
$$(m_1 + m_2) \otimes n = (m_1 \otimes n) + (m_2 \otimes n) \tag{3.13}$$
$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2 \tag{3.14}$$

Example 3.3

We want to show that
$$\mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}_3 = 0$$
We can repeatedly apply (3.12) to $1 \otimes 1$ to see
$$1 \otimes 1 = 1 \cdot 3 \otimes 1 = 1 \otimes 0 = 0 \otimes 0 = 0$$

Proposition 3.12.
$M \otimes_R N$ is an abelian group.

Definition 3.13: Balanced Map.
Let M be a right R-module, N a left R-module and B an abelian group. A function $f : M \times N \to B$ is called R-balanced if :

- ***(a)*** *$f(\cdot, n) : M \to B$ is $\mathbb{Z}$-linear for all $n \in N$.*
- ***(b)*** *$f(m, \cdot) : M \to B$ is $\mathbb{Z}$-linear for all $m \in M$.*
- ***(c)*** *$f(mr, n) = f(m, rn)$ for all $m \in M, n \in N, r \in R$.*

Note that balanced maps are not necessarily homomorphism, but are functions in a groups of one variable.

Theorem 3.14: Universal Mapping Property for Balanced Maps.
Let B be an abelian group, and $\iota : M \times N \to N \otimes N$ be $\iota(m \times n) = m \oplus n$.

Theorem 3.15: Universal Mapping Property for Quotients.
Let B be an abelian group and $A \subset B$ be a subgroup. Let $\pi : B \to B/A$ be $\pi(b) = [b]$. Let A, B, C be abelian groups with $A \subset B$ a subgroup. Let $f : B \to C$ be a map of abelian groups with $f(a) = 0$ for all $a \in A$. Then there exists a unique map of abelian groups $\widehat{f} : B/A \to C$ such that $\widehat{f}(\pi())$

Definition 3.16: Bimodule.
Let R, S be rings and M a left R-module and a right S-module. We say that M is a $R - S$-bimodule if
$$(rm)s = r(ms) \tag{3.15}$$
for all $r \in R$, $m \in M$, and $s \in S$.

Note that if M is a left R-module for a commutative ring R, then M is an R-bimodule with $mr = rm$ for all $r \in R$ and $m \in M$.

Example 3.4

Let J is a two sided ideal in R. Then J is an R-bimodule.

Definition 3.17.
Let M be an $R - S$ bimodule and N a left S-module. Then $M \otimes_S N$ is a left R-module via
$$r(m \otimes n) = (rm) \otimes n \tag{3.16}$$

Corollary 3.18.
If R is commutative, then $M \otimes_R N$ is an R-module.

Example 3.5

Let $R = \mathbb{R}[x]$, $M = \mathbb{R}^2$, and $N = \mathbb{R}$. Let x act on $\mathbb{R}^2$ via $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and x act on $\mathbb{R}$ via $[0]$. We want to find the structure of $\mathbb{R} \otimes_{\mathbb{R}[x]} \mathbb{R}^2$. To do this, we can calculate

$$e_1 \otimes 1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} e_1 \otimes 1 = e_1 x \otimes 1 = e_1 \otimes x1 = e_1 \otimes 0 = 0$$
$$e_2 \otimes 1 = ???$$

Supposedly this generalizes to Proposition 3.19 and we get $\mathbb{R}^2 \otimes_{\mathbb{R}[x]} \mathbb{R}^1 \cong \mathbb{R}^2/\mathrm{im} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cong \mathbb{R}^1$.

Proposition 3.19.
Let V be an $\mathbb{F}$-vector space. $\mathbb{F}[x]$ acts on V via $T : V \to V$ and $\mathbb{F}[x]$ acts on $\mathbb{F}$ via 0. Then

$$V \otimes_{\mathbb{F}[x]} \mathbb{F} \to V/\mathrm{im}\, T = \mathrm{coker}\, T \tag{3.17}$$

and $V \otimes \mathbb{F} \to V/\mathrm{im}\, T$ is a balanced isomorphism.
(This was absolutely not clear in class, prove it on your own)

Proposition 3.20.
Let R be commutative $R \otimes_R M \cong M$

Proposition 3.21.
Let A, B are right M modules and C be a right module.

$$(A \oplus B) \otimes C \cong (A \otimes C) \oplus (B \otimes C) \tag{3.18}$$
$$A \otimes (B \oplus C) \cong (A \otimes B) \oplus (A \otimes C) \tag{3.19}$$

Proposition 3.22.
Let R be a commutative I, J ideals, Then

$$R/I \otimes_R R/J \cong R/I + J \tag{3.20}$$

Proof. Homework 5. □

3.2 Algebra Structures

Definition 3.23.
An R-algebra structure on a ring A is a ring homomorphism $\varphi : R \to A$.

Proposition 3.24.
Let R be a ring and A an R-algebra. Then A is an R-R-bimodule.

Proposition 3.25.
Let R be commutative and A and B be R-algebras. Then $A \otimes_R B$ is a ring with

$$(a \otimes b)(a' \otimes b') = (aa') \otimes (bb') \tag{3.21}$$

Example 3.6

If R is a subring of A, then A is an R-algebra.

Proposition 3.26.
We have

$$R[x] \otimes_R A \cong A[x] \tag{3.22}$$
$$R^n \otimes_R \cong A^n \tag{3.23}$$

Definition 3.27.
Let R be commutative. Let S be multiplicatively closed subset of R containing 1. Then

$$S^{-1}R = R \times S/\sim \tag{3.24}$$

Where $r/s \sim r'/s'$ if $rs't = r'st$ for some $t \in R$.

4 Linear and Multi-Linear Algebra

Definition 4.1.
Let V be an $\mathbb{F}$-vector space. A set $S \subseteq V$ is linearly independent if for all $\vec{v}_1, \ldots, \vec{v}_n \in S$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$, the statement

$$\sum_{i=1}^{n} \alpha_i \vec{v}_i = \vec{0} \tag{4.1}$$

implies all $\alpha_i = 0$.

Proposition 4.2.
S is a basis of V if

- ***(a)*** *$\langle S \rangle = V$*
- ***(b)*** *S is linearly independent.*

Definition 4.3.
$S \subseteq V$ is a basis of V if $F_{\mathbb{F}}(S) \cong V$.

Proposition 4.4.
Let $A \subseteq V$ be finite and assume $\langle A \rangle = V$. Then there exists some $B \subseteq A$ with B being a basis for V.

Lemma 4.5.
Let $\{w_i\}_{i=1}^{m}$ be a basis of $W \subseteq V$. Then tehre are $v_{m+1}, \ldots v_n$ with $\{w_i\}$ as a basis.

Definition 4.6.
We define the dimension of a vector space V to be $\dim V = n$ if $V \cong \mathbb{F}^n$.

Proposition 4.7.
If $\dim V = \dim W < \infty$ then $V \cong W$.

Proposition 4.8.
Let $W \subseteq V$ be a subspace, then

$$\dim V = \dim W + \dim V/W \tag{4.2}$$

Corollary 4.9: Rank-Nullity Theorem.
Let $\varphi : V \to U$ be $\mathbb{F}$-linear. Then

$$\dim V = \dim \ker \varphi + \dim \operatorname{im} \varphi \tag{4.3}$$

Proposition 4.10.
Let $\varphi : V \to W$. The following are equivalent:

- ***(a)*** *φ is an isomorphism*
- ***(b)*** *φ is injective*
- ***(c)*** *φ is surjective*
- ***(d)*** *φ sends a basis of V to a basis of W.*

Definition 4.11: Dual Space.
Let V be an $\mathbb{F}$-vector space. Let $V^* = \hom(V, \mathbb{F})$.

Proposition 4.12.
If $\dim V < \infty$, then $V \cong V^*$.

Proof. Let $\dim V = n$. Then $V \equiv \mathbb{F}^n$ and we can say that

$$\hom_{\mathbb{F}}(V, \mathbb{F}) \cong \hom_{\mathbb{F}}(\mathbb{F}^n, \mathbb{F}) \cong \mathrm{Mat}_{\mathbb{F}}(1, n) \cong \mathbb{F}^n \tag{4.4}$$

by Theorem **??** ☐

Definition 4.13.
If $\vec{v}_1, \dots, \vec{v}_n$ is a basis of v, let $\vec{v}_i^*$ be

$$\vec{v}_1^* \left(\sum_j a_j \vec{v}_j \right) = a_j \tag{4.5}$$

where we can also say

$$\vec{v}_i^*(\vec{v}_j) = \delta_{ij} \tag{4.6}$$

where δ_{ij} is the Kronecker delta.

Note that there is an isomorphism from $v_i \mapsto v_i^*$ if $\dim V < \infty$.

Proposition 4.14.
If $a_1, \dots, a_n$ is a basis of V, and $b_1, \dots, b_m$ are linearly independent, then $m \leq n$ and $b_1, \dots, b_m, a_{m+1}, \dots a_n$ is a basis of V after the proper reordering of indices.

Corollary 4.15.
If $W \subseteq V$, then $\dim W \leq \dim V$.

Proof. Any basis $b_1, \dots, b_n$ of W is linearly independent, so apply Proposition 4.14 on a basis $a_1, \dots, a_n$ of V, to see that the basis of V has at least as many elements as the basis of W. □

Note that if $\dim W = \dim V$, then $W = V$.

Definition 4.16.
Let $\alpha = \{\vec{a}_i\}_1^n$ be a basis of V and $\beta = \{\vec{b}_i\}_1^n$ be a basis of W. For $T : V \to W$ linear, let

$$M_\beta^\alpha(\varphi) = \begin{bmatrix} r_{11} & \dots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{m1} & \dots & r_{mn} \end{bmatrix} \tag{4.7}$$

With

$$T(\vec{a}_j) = \sum_{i=1}^n r_{ij} \vec{b}_i \tag{4.8}$$

Proposition 4.17.
Let $\varphi, \psi : V \to W$. If $M_\beta^\alpha(\varphi) = M_\beta^\alpha(\psi)$, the $\varphi = \psi$.

Proposition 4.18.
Let M be $m \times n$. Pick bases α on V and β on W. Let $\varphi_\alpha^\beta : V \to W$ be

$$\varphi_\alpha^\beta \left(\sum_i s_i \vec{a}_i \right) = \sum_i \sum_j s_i r_{ij} \vec{b}_j \tag{4.9}$$

Note that φ_α^β is well-defined and a linear map.

Definition 4.19: Adjoint Map.
Let $T : V \to W$ and $T^* : W^* \to V^*$ be $f \in W^*$ with $f : W \to \mathbb{F}$. Let $T^*(f) \in V^*$ be

$$T^*(f)(\vec{v}) = f(T(\vec{v})) \tag{4.10}$$

Definition 4.20: Symmetric Group.
Define the Symmetric group on n elements by

$$S_n = \{f : \{1, \dots, n\} \to \{1, \dots, n\} | f \text{ is bijective}\} \tag{4.11}$$

Example 4.1

Define the following:

$$\sigma: \quad 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1 \tag{4.12}$$
$$\tau: \quad 1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 3 \tag{4.13}$$

and define

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \tag{4.14}$$

Then

$$\sigma(\Delta) = (x_2 - x_1)(x_2 - x_1)(x_2 - x_1) \tag{4.15}$$
$$= (x_2 - x_3)(-1)(x_1 - x_2)(-1)(x_1 - x_3) \tag{4.16}$$
$$= \Delta \tag{4.17}$$

and

$$\tau(\Delta) = -\Delta \tag{4.18}$$

by the same logic. The goal of this example is to define the sgn function.

Proposition 4.21.
For all $\sigma \in S_n$, we have

$$\sigma(\Delta) = \pm\Delta \tag{4.19}$$

Definition 4.22: Sign Function.
Let $\operatorname{sgn}: S_n \to \{\pm 1\}$ *be*

$$\operatorname{sgn}(\sigma) = \frac{\sigma(\Delta)}{\Delta} = \begin{cases} 1 & \text{if } \sigma(\Delta) = \Delta \\ -1 & \text{if } \sigma(\Delta) = -\Delta \end{cases} \tag{4.20}$$

Proposition 4.23.
sgn *is a homomorphism.*

Proposition 4.24.
$\operatorname{sgn}: S_n \to \{\pm 1\}$ *is surjective for all* $n \geq 2$.

Definition 4.25.
Let

$$A_n = \ker(S_n \to \{\pm 1\}) \tag{4.21}$$

Definition 4.26.
Let $A = (a_{ij}) \in \mathrm{Mat}_{\mathbb{F}}(n,n)$. *Then*

$$\det(A) = \sum_{r \in S_n} \operatorname{sgn}(\sigma) a_{a\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)} \tag{4.22}$$

Theorem 4.27.
We have that the determinant defined as

$$\det: \mathrm{Mat}_{\mathbb{F}}(n,n) \to \mathbb{F} \tag{4.23}$$

is the unique alternating n-linear function sending $\mathbb{I} \mapsto 1$

Note that we often identify $(\mathbb{F}^n)^n \cong \mathrm{Mat}_{\mathbb{F}}(n,n)$.

Definition 4.28.
For $-1 \neq 1 \in \mathbb{F}$, we say

$$f : V \times \cdots \times V \to W \tag{4.24}$$

is alternating if $f(\vec{v}_1, \ldots, \vec{v}_n) = \operatorname{sgn}(\sigma) f(\vec{v}_{\sigma(1)}, \ldots, \vec{v}_{\sigma(n)})$ for all $\sigma \in S_n$.

Example 4.2

The usual 3-dimensional cross product defined as

$$\times : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3 \qquad (\vec{v}, \vec{w}) \mapsto \vec{v} \times \vec{w}$$

is alternating.

Proposition 4.29.
The determinant as defined in Theorem 4.27 is alternating.

Proposition 4.30.
The determinant is n-linear and $\det \mathbb{I}_n = 1$ for all n.

Proposition 4.31.
If $f : \mathbb{F}^{m_1} \times \cdots \times \mathbb{F}^{m_n} \to W$ is n-linear, then f is determined by its values on $(e_{i_1}, \ldots, e_{i_n})$.

Proof. See Example 4. □

Example 4.3

Define $f : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ and let

$$\begin{aligned} f(e_1, e_1) &= 2 \\ f(e_1, e_2) &= 3 \\ f(e_2, e_1) &= 4 \\ f(e_2, e_2) &= 0 \end{aligned}$$

What is $f\left(\begin{bmatrix} c \\ d \end{bmatrix}, \begin{bmatrix} a \\ b \end{bmatrix}\right)$? We see

$$\begin{aligned} f\left(\begin{bmatrix} c \\ d \end{bmatrix}, \begin{bmatrix} a \\ b \end{bmatrix}\right) &= f(ae_1 + be_2, ce_1 + de_2) \\ &= af(e_1, ce_1 + de_2) + baf(e_2, ce_1 + de_2) \\ &= acf(e_1, e_1) + adf(e_1, e_2) + bcf(e_2, e_1) + bdf(e_2, e_2) \\ &= 2ac + 3ad + 4bc \end{aligned}$$

The proof of Proposition 4.31 is given by the same computation in more general terms.

Proposition 4.32.
$\det(A) = \det(A^T)$.

Theorem 4.33: Expansion by Minors.
We can expand the determinant in the following way:

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}) \tag{4.25}$$

$$= \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}) \tag{4.26}$$

$$
\begin{tikzcd}
M_1 \times M_2 \arrow[r, "f"] \arrow[d] & W \\
M_1 \otimes_R M_2 \arrow[ur, "\widehat{f}"] &
\end{tikzcd}
$$

Figure 4

Theorem 4.34.
Let R be commutative, and f bilinear. Then there exists a unique $\widehat{f}$ which is linear and makes the diagram in Figure 4 commute.

This theorem generalizes to k elements.

Definition 4.35.
Define

$$\operatorname{sym}^k(M) = (M \otimes_R \cdots \otimes_R M)/N \tag{4.27}$$

where

$$N = \left\langle (m_1 \otimes \cdots \otimes m_k) - \left(m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)}\right)\right\rangle \tag{4.28}$$

Then we have

$$\operatorname{Sym}(M) = \bigoplus_k \operatorname{Sym}^k(M) \tag{4.29}$$

Definition 4.36.
We say that $f : M^k \to W$ is symmetric if

$$f(m_1, \ldots, m_k) = f(m_{\sigma(1)}, \ldots, m_{\sigma(k)}) \tag{4.30}$$

for all $\sigma \in S_k$.

Theorem 4.37.
Let R be commutative, and $f : M^k \to W$ be k-linear and symmetric. Then there exists a unique $\widehat{f}$ which is linear and makes the diagram in Figure 5 commute.

$$
\begin{tikzcd}
M^k \arrow[r, "f"] \arrow[d] & W \\
\operatorname{Sym}^k M \arrow[ur, "\widehat{f}"] &
\end{tikzcd}
$$

Figure 5

4.1 An Excursion into Multivariate Calculus

Definition 4.38.
Assume $1 \neq -1 \in R$. Then

$$\wedge^k M = M^{\otimes k} / \left\langle m_1 \otimes \cdots \otimes m_k + m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)} \right\rangle \tag{4.31}$$

Example 4.4

$$a \wedge b = -(b \wedge a)$$

Theorem 4.39.
We define

$$\dim_{\mathbb{F}} \wedge^k \mathbb{F}^n = \binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{4.32}$$

and $S = \{e_{n_1} \wedge \cdots \wedge e_{n_k}\}$ *is a basis for* $n_i < n_{i+1}$.

Definition 4.40: Cross Product.
We can define

$$\times : \mathbb{R}^3 \times \mathbb{R}^3 \to (\mathbb{R}^3)^{\otimes 2} \to \wedge^2 \mathbb{R}^2 \cong \mathbb{R}^3 \tag{4.33}$$

as our cross product in 3 dimensions.

Definition 4.41.
Let $f : \mathbb{R}^n \to \wedge^k \mathbb{R}^n$. *Then we define* $df : \mathbb{R}^n \to \wedge^{k+1} \mathbb{R}^n$ *as*

$$g(e_{n_1} \wedge \cdots \wedge e_{n_k}) \mapsto \sum_i \frac{\partial g}{\partial x_i} e_i \wedge e_{n_1} \wedge \cdots \wedge e_{n_k} \tag{4.34}$$

for some $g : \mathbb{R}^n \to \mathbb{R}$.

The upshot of this definition is that in $\mathbb{R}^3$ the function $f : \mathbb{R}^3 \to \wedge^1 \mathbb{R}^3$ is a vector field and df is the curl of f. If instead$f : \mathbb{R}^3 \to \wedge^2 \mathbb{R}^3$, df becomes the divergence.

5 Matrix Algebra

Definition 5.1.
Let $T"V \to W$ be linear and $\widehat{T} : \wedge^k V \to \wedge^k W$ be

$$\widehat{T}(v_1 \wedge \cdots \wedge v_k) = T(v_1) \wedge \cdots \wedge T(v_k) \tag{5.1}$$

Proposition 5.2.
$\widehat{T}$ is linear and well defined. Furthermore, we have that if $T : \mathbb{F}^n \to \mathbb{F}^n$ has matrix A. Then

$$\widehat{T}(e_1 \wedge \cdots \wedge e_n) = \det(A) e_1 \wedge \cdots \wedge e_n \tag{5.2}$$

Definition 5.3.
Let $T : V \to V$ where $\dim V = n$. Then $\det(T) = a \in \mathbb{F}$ if $\widehat{T} : \wedge^n V \to \wedge^n V$ is defined by multiplication by a.

Proposition 5.4.
Let $T : V \to W$ and $S : w \to U$. Then

$$\widehat{S} \circ \widehat{T} = (\widehat{S \circ T}) : \wedge^k V \to \wedge^k U \tag{5.3}$$

Corollary 5.5.
If $S, T : V \to V$, then

$$\det(S \circ T) = \det(S)\det(T) \tag{5.4}$$

Corollary 5.6.

$$\det(T^{-1}) = \frac{1}{\det(T)} \tag{5.5}$$

Proof.

$$1 = \det(\mathbb{I}) = \det(TT^{-1}) = \det(T)\det(T^{-1})$$

□

Corollary 5.7.
If $\det(T) = 0$, then T is not invertible.

Proposition 5.8.
If $T : V \to V$ is not invertible, then $\det T = 0$.

Theorem 5.9.
Let $\mathbb{F}^n \cong_{\mathbb{F}[x]} \operatorname{coker}(\mathbb{F}[x]^n \to \mathbb{F}[x]^n)$. Then $A - xI$ is row or column wise diagonalizable, such that $a_1(x) | a_2(x) | \ldots | a_n(x)$ and

$$\mathbb{F}^n \cong \bigoplus_{i=1}^{n} \mathbb{F}[x]^n / a_i(x) \tag{5.6}$$

Proposition 5.10.
Let $V = \mathbb{F}[x]/p(x)$ where $p(x)$ is a monic polynomial of degree d with coefficents r_i. Let $T : V \to V$ be multiplication by x. Then $\{1, x, x^2, \ldots, x^{d-1}\}$ is a basis of V and the matrix of T with respect to this basis is

$$\begin{bmatrix} 0 & 0 & 0 & \ldots & -r_0 \\ 1 & 0 & 0 & \ldots & -r_1 \\ 0 & 1 & 0 & \ldots & -r_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & -r_{d-1} \end{bmatrix} \tag{5.7}$$

Definition 5.11: Jordan Block.
We define the Jordan block of size d, by

$$J_d(\lambda) = \begin{bmatrix} \lambda & 1 & & & & & \\ & \lambda & 1 & & & & \\ & & \lambda & 1 & & & \\ & & & \lambda & 1 & & \\ & & & & \ddots & \ddots & \\ & & & & & \lambda & 1 \end{bmatrix} \tag{5.8}$$

Theorem 5.12.
If $P_A(x)$ splits, then

$$A \sim \begin{bmatrix} J_{d_1}(\lambda_1) & & \\ & J_{d_2}(\lambda_2) & \\ & & \ddots \end{bmatrix} \tag{5.9}$$

which is Jordan Normal form.

Proposition 5.13.
For A_i square, we have

$$\begin{bmatrix} A_1 & & \\ & A_2 & \\ & & \ddots \end{bmatrix}^k = \begin{bmatrix} A_1^k & & \\ & A_2^k & \\ & & \ddots \end{bmatrix} \tag{5.10}$$

Using this proposition, we can seeing how we can raise any matrix to a high power, and easily calculate it use Jordan normal form.

Proposition 5.14.

$$[J_d(\lambda)]^k = \begin{bmatrix} \lambda^k & k\lambda^{k-1} & \binom{k}{2}\lambda^{k-2} & \cdots & \binom{k}{d}\lambda^{k-d} \\ & \lambda^k & k\lambda^{k-1} & \cdots & \binom{k}{d-1}\lambda^{k-(d-1)} \\ & & \lambda^k & \cdots & \binom{k}{d-2}\lambda^{k-(d-2)} \\ & & & \ddots & \vdots \\ & & & & \lambda^k \end{bmatrix} \tag{5.11}$$

Definition 5.15.
We say that λ is an eigenvalue of A if $A\vec{v} = \lambda\vec{v}$ for $\vec{v} \neq \vec{0}$. We say that $\vec{v}$ is its associated eigenvector.

Definition 5.16.
The space of eigenvectors for an eigenvalue λ is given by

$$E_\lambda = \ker(A - \lambda I) \tag{5.12}$$

For consistency, we say that $E_\lambda \setminus \{\vec{0}\}$ are all of the (nontrivial) λ eigenvectors.

We can now use Jordan normal form to determine the number of eigenvalues of a matrix with the following proposition:

Proposition 5.17.
If $P_A(x)$ splits, then $\dim E_\lambda$ is equal to the number of λ Jordan blocks.

Definition 5.18: Generalized Eigenvector.
Let $\vec{v}_1$ be a λ-eigenvector For $j \geq 2$, solve $A\vec{v}_j = \lambda\vec{v}_j + \vec{v}_{j-1}$, we say that $\vec{v}_j$ is a depth j generalized eigenvector associated to $\vec{v}_1$¿

Theorem 5.19.
Assume $P_A(x)$ splits. Let $B = \{b_1, \ldots, b_n\}$ be a maximal linearly independent set of generalized eigenvectors. Then $A = BJB^{-1}$ with J in Jordan Normal Form and B is some $B = [b_1, \ldots, b_n]$. Note that the b_i may have to be normal to determine J in JNF.

6 Spectral Theory

Definition 6.1.
Let $f_A : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}$ is

$$f_A(\vec{v}, \vec{w}) = \vec{v} \cdot (A\vec{w}) \tag{6.1}$$

We say f is alternating if $f(\vec{v}, \vec{w}) = -f(\vec{w}, \vec{v})$ and symmetric if $f(\vec{v}, \vec{w}) = f(\vec{w}, \vec{v})$.

Example 6.1

Suppose $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then

$$f_A\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}, [1, 0]\right) = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = a$$

If f_A is alternating, then $a = 0$ and $d = 0$, so $A = -A^T$. If f_A is symmetric, then $A = A^T$.

This example gives us equivalent definitions to symmetric and alternating matrices in the form of the following proposition:

Proposition 6.2.
Assume we are not in a field of characteristic 2. Then f_A is symmetric if and only if A is symmetric and f_A is alternating if and only if A is anti-symmetric.

Definition 6.3: Inner Product.
Let V be an $\mathbb{R}$-vector space. Then $f : V \times V \to \mathbb{R}$ is an inner product if:

(a) *f is bilinear.*

(b) *f is symmetric.*

(c) *$f(\vec{v}, \vec{v}) \geq 0$ for all $\vec{v} \neq 0$.*

Example 6.2

Take $A = \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$. The natural question arises: is f_A an inner product? The eigenvalues of A are 5 and 3, and the corresponding eigenvector to 3 is negative, so it cannot be an inner product.

Theorem 6.4: Spectral Theorem.
Let $A \in \mathrm{Mat}_{\mathbb{R}}(n, n)$ be symmetric. Then there exists a $B \in \mathrm{Mat}_{\mathbb{R}}(n, n)$ with

(a) *BAB^{-1} diagonal.*

(b) *$B^T = B^{-1}$.*

Corollary 6.5.
If A is symmetric and real, then A is diagonalizable with real eigenvalues.

Corollary 6.6.
f_A is an inner product on $\mathbb{R}^n$ if and only if A is symmetric all eigenvalues are positive.

Proposition 6.7.
Let $f : V \times V \to \mathbb{R}$ be an inner product. Then f is non-degenerate.

Definition 6.8.
$f : V \times V \to \mathbb{F}$ is bilinear. Let $f^* : V \to V^*$.be

$$v \mapsto (w \mapsto f(\vec{v}, \vec{w})) \tag{6.2}$$

Then f is non-degenerate if f^* is an isometry.

Definition 6.9.
Let (V, f) and (W, g) be inner product spaces. Then $T : V \to W$ is an isometry if

(a) *T is an isomorphism.*

(b) *$g(T(\vec{v}), T(\vec{w})) = f(\vec{v}, \vec{w})$.*

References

[1] David S. Dummit and Richard M. Foote. *Abstract Algebra*. 3rd ed. New York: Wiley, 2004.

[2] Kenneth M. Hoffman and Ray Kunze. *Linear Algebra*. 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 1971.