Honours Algebra Notes

Leon Lee

March 25, 2024

Contents

1 Vector Spaces

1.1 Fields and Vector Spaces

Definition 1.1.1: Definition of a field

A **field** F is a set with functions

- Addition: $+ : F \times F \to F$, $(\lambda, \mu) \mapsto \lambda + \mu$
- Multiplication: $\cdot : F \times F$, $(\lambda, \mu) \mapsto \lambda\mu$

and two distinguished members 0_F, 1_F with $0_F \neq 1_F$ s.t. $(F, +)$ and $F \backslash \{0_F, \cdot\}$ are *abelian groups* whose neutral elements are 0_F and 1_F respectively, and which also satisifies

$$\lambda(\mu + \nu) = \lambda\mu + \lambda\nu \in F$$

for any $\lambda, \mu, \nu \in F$. Additional Requirements: For all $\lambda, \mu \in F$,

- $\lambda + \mu = \mu + \lambda$
- $\lambda \cdot \mu = \mu \cdot \lambda$
- $\lambda + 0_F = \lambda$
- $\lambda \cdot 1_F = \lambda \in F$

For every $\lambda \in F$ there exists $-\lambda \in F$ such that

$$\lambda + (-\lambda) = 0_F \in F$$

For every $\lambda \neq 0 \in F$ there exists $\lambda^{-1} \neq 0 \in F$ such that

$$\lambda(\lambda^{-1}) = 1_F \in F$$

NOTE: This is a terrible definition of a field, just think of it as a group with two operations instead of one

Definition 1.1.2: Definition of a Vector Space

A **vector space** V **over a field** F is a pair consisting of an abelian group $V = (V, \dot{+})$ and a mapping

$$F \times V \to V : (\lambda, \vec{v}) \mapsto \lambda\vec{v}$$

such that for all $\lambda, \mu \in F$ and $\vec{v}, \vec{w} \in V$ the following identities hold:

$$\begin{aligned} \lambda(\vec{v} \dot{+} \vec{w}) &= (\lambda\vec{v}) \dot{+} (\lambda\vec{w}) \\ (\lambda + \mu)\vec{v} &= (\lambda\vec{v}) \dot{+} (\mu\vec{v}) \\ \lambda(\mu\vec{v}) &= (\lambda\mu)\vec{v} \\ 1_F\vec{v} &= \vec{v} \end{aligned}$$

The first two laws are the **Distributive Laws**, the third law is called the **Associativity Law**. A vector field V over a field F is commonly called an **F-vector space**

1.1.3 Vector Space Terminology

- Elements of a vector space: **vectors**
- Elements of the field F: **scalars**
- The field F itself: **ground field**
- The map $(\lambda, \vec{v}) \mapsto \lambda\vec{v}$: **multiplication by scalars**, or the **action of the field F on V**

Notes:

- This is not the same as the "scalar product", as that produces a scalar from two vectors
- Let the zero element of the abelian group V be written as $\vec{0}$ and called the **zero vector**
- The use of $\dot{+}$ and 1_F is there for mostly pedantic rigorous reasons, and a much less confusing way of defining a vector field is defined below:

Definition 1.1.4: Alternative Vector Space definition

A **vector space V over a field F** is a pair consisting of an abelian group $V = (V, \dot{+})$ and a mapping

$$F \times V \to V : (\lambda, \vec{v}) \mapsto \lambda\vec{v}$$

such that for all $\lambda, \mu \in F$ and $\vec{v}, \vec{w} \in V$ the following identities hold:

$$\begin{aligned} \lambda(\vec{v} \dot{+} \vec{w}) &= \lambda\vec{v} \dot{+} \lambda\vec{w} \\ (\lambda + \mu)\vec{v} &= \lambda\vec{v} \dot{+} \mu\vec{v} \\ \lambda(\mu\vec{v}) &= (\lambda\mu)\vec{v} \\ 1\vec{v} &= \vec{v} \end{aligned}$$

1.1.5 Vector Space Lemmas

Product with the scalar zero: If V is a *vector space* and $\vec{v} \in V$, then $0\vec{v} = \vec{0}$, or in words "zero times a vector is the zero vector"
Product with the scalar (-1): If V is a *vector space* and $\vec{v} \in V$, then $(-1)\vec{v} = -\vec{v}$
Product with the zero vector: If V is a *vector space* over a field F, then $\lambda\vec{0} = \vec{0}$ for all $\lambda \in F$. Furthermore, if $\lambda\vec{v} = \vec{0}$ then either $\lambda = 0$ or @$\vec{v} = \vec{0}$

1.2 Product of Sets and of Vector Spaces

Definition 1.2.1: Cartesian Product of n sets

Trivially: $X \times Y = \{(x, y) : x \in X,\, y \in Y\}$
Just extend this to n numbers

$$X_1 \times \cdots \times X_n := \{(x_1, \ldots, x_n) : x_i \in X_i \text{ for } 1 \leq i \leq n\}$$

The elements of a product are called **n-tuples**. An individual entry $x_i = (x_1, \ldots, x_n)$ is called a **component**.
There are special mappings called **projections** for a cartesian product:

$$\begin{aligned} \mathrm{pr}_i : X_1 \times \cdots \times X_n &\to X_i \\ (x_1, \ldots, x_n) &\mapsto x_i \end{aligned}$$

The cartesian product of n copies of a set X is written in short as: X^n

The elements of X^n are n-tuples of elements from X. In the special case $n = 0$ we use the general convention that X^0 is "the" one element set, so that for all $n, m \geq 0$, we then have the canonical bijection

$$\begin{aligned} X^n \times X^m &\to X^{n+m} \\ ((x_1, x_2, \ldots, x_n),\, (x_{n+1}, x_{n+2}, \ldots, x_{n+m})) &\mapsto (x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m}) \end{aligned}$$

Note: the $\to$ should have a tilde but idk how to typeset it like that
[Bunch of examples: check LN 1.3]

1.3 Vector Subspaces

Definition 1.3.1: Vector Subspace

A subset U of a vector space V is called a **vector subspace** or **subspace** if U contains the zero vector, and whenever $\vec{u}, \vec{v} \in U$ and $\lambda \in F$ we have $\vec{u} + \vec{v} \in U$ and $\lambda\vec{u} \in U$

Note There is a more generalized definition using concepts we haven't learned yet, it is as follows: Let F be a field. A subset of an F-vector space is called a vector subspace if it can be given the structure of an F-vector space such that the embedding is a "homomorphism of F-vector spaces". This definition is a lot more general since it also applies to subgroups, subfields, sub-"any structure", etc

Definition 1.3.2: Spanning Subspace

Let T be a subset of a vector space V over a field F. Then amongst all vector subspaces of V that include T there is a smallest vector subspace

$$\langle T \rangle = \langle T \rangle_F \subseteq V$$

It can be described as the set of all vectors $\alpha_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r$ with $\alpha_1, \ldots, \alpha_r \in F$ and $\vec{v}_1, \ldots, \vec{v}_r \in T$, together with the zero vector in the case $T = \emptyset$

1.3.3 Subspace terminology

- An expression of the form $a_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r$ is called a **linear combination** of vectors $\vec{v}_1, \ldots, \vec{v}_r$.
- The smallest vector subspace $\langle T\rangle \subseteq V$ containing T is called the **vector subspace generated by** T or the vector subspace **spanned by** T or even the **span of** T
- If we allow the zero vector to be the "empty linear combination of $r = 0$ vectors", which is what we will mean from hereon, then the span of T is exactly the set of all linear combinations of vectors from T

Definition Number: Generating Subspace

A subset of a vector space is called a **generating** or **spanning set** of our vector space if its span is all of the vector space. A vector space that has a finite generating set is said to be **finitely generated**.

1.4 Linear Independence and Bases

Definition 1.4.1: Linear Independence

A subset L of a vector space V is called **linearly independent** if for all pairwise different vectors $\vec{v}_1, \ldots, \vec{v}_r \in L$ and arbitrary scalars $\alpha, \ldots, \alpha_r \in F$,

$$a_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r = \vec{0} \implies a_1 = \cdots = \alpha_r = 0$$

Definition 1.4.2: Linear Dependence

A subset L of a vector space V is called **ilnearly dependent** if it is not linearly independent (duh..). This means there exists pairwise different vectors $\vec{v}j_1, \ldots, \vec{v}_r \in L$ and scalars $\alpha_1, \ldots, \alpha_r \in F$, not all zero, such that $\alpha_1\vec{v}_1 + \cdots \alpha_r\vec{v}_r = \vec{0}$

Definition 1.4.3: Basis of a Vector Space

A **basis of a vector space** V is a linearly independent generating set in V

1.4.4 Family notation

Let A and I be sets. We will refer to a mapping $I \to A$ as a **family of elements of A indexed by** I and use the notation

$$(a_i)i \in I$$

This is used mainly when I plays a secondary role to A. In the case $I = \emptyset$, we will talk about the **empty family** of elements of A.
Random facts:

- The family $(\vec{v}_i)_{i\in I}$ would be called a generating set if the set $\{\vec{v}_i : i \in I\}$ is a generating set.
- It would be called **linearly independent** or a **linearly independent family** if, for pairwise distinct indices $i(1), \ldots, i(r) \in I$ and arbitrary scalars $a_1, \ldots, a_r \in F$,

$$a_1\vec{v}_{i(1)} + \cdots + a_r\vec{v}_{i(r)} = \vec{0} \to \alpha_1 = \cdots = a_r = 0$$

A difference between families and subsets is that the same vector can be represented by different indices in a family, in which case linear independence as a family is not possible. A family of vectors that is not linearly independent is called a **linearly dependent family**. A family of vectors that is a generating set and linearly independent is called either a **basis** or a **basis indexed by** $i \in I$

Example 1.4.5: Standard Basis

Let F be a field and $n \in \mathbb{N}$. We consider the following vectors in F^n

$$\vec{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$$

with one 1 in the i-th place and zero everywhere else. Then $\vec{e}_1, \ldots, \vec{e}_n$ form an ordered basis of F^n, the so-called **standard basis of** F^n

Theorem 1.4.6: Linear combinations of basis elements

Let F be a field, V a vector space over F and $\vec{v}_1, \ldots, \vec{v}_r \in V$ vectors. The family $(\vec{v}_i)_{1 \leq i \leq r}$ is a basis of V if and only if the following "evaluation" mapping

$$\begin{aligned} \psi : F^r &\to V \\ (\alpha_1, \ldots, a_r) &\mapsto a_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r \end{aligned}$$

is a bijection

If we label our ordered family by $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_r)$, then we done the above mapping by

$$\psi = \psi_{\mathcal{A}} : F^r \to V$$

2 Rings

I can't be bothered doing changes of basis and stuff, time for something more interesting :D

2.1 Ring basics

Definition 2.1.1: Definition of a Ring

A **ring** is a set with two operations $(\mathbb{R}, +, \cdot)$ that satisfy:

1. $(R, +)$ is an abelian group
2. $(R, \cdot)$ is a **monoid** - this means that the second operation $\cdot : R \times R \to R$ is associative and that there is an **identity element** $1 = 1_R \in R$, often just called the identity, with the property that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.
3. The distributive laws hold, meaning that for all $a, b, c \in R$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c))$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

The two operations are called **addition** and **multiplication** in our ring. A ring in which multiplication, that is $a \cdot b = b \cdot a$ for all $a, b \in R$, is a **commutative ring**

Note: We'll call the element $1 \in R$ as the identity element of the monoid $(R, \cdot)$, and we call the additive identity of $(R, +)$ zero, written as 0_R or 0
Example: We can define the **null ring** or **zero ring** as a ring where R is a single ement set, e.g. $\{0\}$, with the operations $0 + 0 = 0$ and $0 \times 0 = 0$. We will call any ring that isn't the zero ring a **non-zero ring**

Example 2.1.2: Modulo Rings

Let $m \in \mathbb{Z}$ be an integer. Then the set of **integers modulo** m, written

$$\mathbb{Z}/m\mathbb{Z}$$

is a ring. The elements of $\mathbb{Z}/m\mathbb{Z}$ consist of **congruence classes** of integers modulo m - that is the elements are the subsets T of $\mathbb{Z}$ of the form $T = a + m\mathbb{Z}$ with $a \in \mathbb{Z}$. Think of these as the set of integers that have the same remainder when you divide them by m. I denote the above congruence class by $\overline{a}$. Obviously $\overline{a} = \overline{b}$ is the same as $a - b \in m\mathbb{Z}$, and often I'll write

$$a \equiv b \mod m$$

If $m \in \mathbb{N}_{\geq 0}$ then there are m congruence classes modulo m, in other words, $|\mathbb{Z}/m\mathbb{Z}| = m$, and I could write out the set as

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

To define addition and multiplication, set

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{and} \quad \overline{a} \cdot \overline{b} = \overline{ab}$$

Distributivity for $\mathbb{Z}/m\mathbb{Z}$ then follows from distributivity for $\mathbb{Z}$.

2.2 Linking Rings to Fields and Further Properties

Definition 2.2.1: Ring definition of a field

A **field** is a non-zero commutative ring F in which every non-zero element $a \in F$ has an inverse $a^{-1} \in F$, that is an element a^{-1} with the property that $a \cdot a^{-1} = a^{-1} \cdot a = 1$

Example: The ring $\mathbb{Z}/3\mathbb{Z}$ is a field, which we have been calling $\mathbb{F}_3$. The ring $\mathbb{Z}/12\mathbb{Z}$ is not a field, because neither $\overline{3}$ or $\overline{8}$ are invertible, since $\overline{3} \cdot \overline{8} = \overline{0}$.

Theorem 2.2.2: Prime property of fields

Let m be a positive integer. The commutative ring $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime.

Theorem 2.2.3: Lemmas for multiplying by zero and negatives

Let R be a ring and let $a, b \in R$. Then

1. $0a = 0 = a0$
2. $(-a)b = -(ab) = a(-b)$
3. $(-a)(-b) = ab$

Note: The distributive axiom for rings has familiar properties such as

$$(a+b)(c+d) = ac + ad + bc + bd$$
$$a(b-c) = ab - ac$$

But remember that multiplication is not always commutative, so multiplicative factors must be kept in the correct order - ac may not equal ca

---

Suppose we have a ring R such that $1_R = 0_R$, then R must be the zero ring. 3.2.2 in notes for proof

Definition 2.2.4: Multiples of an abelian group

Let $m \in \mathbb{Z}$. The m**-th multiple** ma **of an element** $a$in an abelian group R is:

$$ma = \underbrace{a + a + \cdots + a}_{m \text{ terms}} \quad \text{if} m > 0$$

$0a = 0$ and negative multiples are defined by $(-m)a = -(ma)$

Theorem 2.2.5: Lemmas for multiples

Let R be a ring, let $a, b \in R$ and let $m, n \in \mathbb{Z}$. Then:

1. $m(a+b) = ma + mb$
2. $(m+n)a = ma + na$
3. $m(na) = (mn)a$
4. $m(ab) = (ma)b = a(mb)$
5. $(ma)(nb) = (mn)(ab)$

Proof. (in the lecturer's words) This is trivial and boring, so I will leave the details up to you. $\square$

Definition 2.2.6: Unit of a ring

Let R be a ring. An element $a \in R$ is called a **unit** if it is *invertible* in R or in other words *has a multiplicative inverse in* R, meaning that there exists $a^{-1} \in R$ such that

$$aa^{-1} = 1 = a^{-1}a$$

Example: In a field, such as $\mathbb{R}, \mathbb{R}, \mathbb{C}$, every non-zero element is a unit. In $\mathbb{Z}$, only 1 and -1 are units

Theorem 2.2.7: The subset of units in a ring forms a group

The set $R^\times$ of units in a ring R forms a group under multiplication

I will call $R^\times$ the **group of units of the ring** R

Definition 2.2.8: zero-divisors of a ring

In a ring R, a non-zero element a is called a **zero-divisor** or **divisor of zero** if there exists a non-zero element b such that either $ab = 0$ or $ba = 0$.

Example: In $\mathrm{Mat}(2; \mathbb{R})$,

$$\begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

So, both $\begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ are zero-divisors

Definition 2.2.9: Integral Domain

An **integral domain** is a non-zero commutative ring that has no zero-divisors.
In an integral domain there are no zero-divisors and therefore the following laws will hold:

1. $ab = 0 \implies a = 0$ or $b = 0$, and
2. $a \neq 0$ and $b \neq 0 \implies ab \neq 0$

Example: $\mathbb{Z}$ is an integral domain. Any field is an integral domain, since a unit in a ring R cannot be a zero-divisor. To see this, let R be a non-zero ring and let $a \in R^\times$ be a unit. Suppose that $ab = 0$ or $ba = 0$ for some $b \in R$. Multiplying on the left or on the right respectively by a^{-1} shows that $a^{-1}ab = a^{-1}0$ or $baa^{-1} = 0a^{-1}$, so in both cases, $b = 0$

Theorem 2.2.10: Cancellation Law for Integral Domains

Let R be an *integral domain* and let $a, b, c \in R$. If $ab = ac$ and $a \neq 0$ then $b = c$

We will now reprove 2.2.2 as a special case of a general theorem

Theorem 2.2.11: Prime Property for Integral Domains

Let m be a natural number. Then $\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if m is prime.

Theorem 2.2.12: Finite Integral Domains are Fields

Every **finite** integral domain is a field.

2.3 Polynomials

Definition 2.3.1: Polynomial

Let R be a ring. A **polynomial over** R is an expression of the form

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$$

for some non-negative integer m and elements $a_i \in R$ for $0 \leq i \leq m$. The set of all polynomials over R is denoted by $R[X]$. In the case where a_m is non-zero, the polynomial P has **degree** m, (written $\deg(P)$), and a_m is its **leading coefficient**. When the leading coefficient is 1 the polynomial is a **monic polynomial**. A polynomial of degree one is called **linear**, a polynomial od degree two is called **quadractic**, and a polynomial of degree three is called **cubic**.

Definition 2.3.2: Ring of Polynomials

The set $R[X]$ becomes a ring called the **ring of polynomials with coefficients in** R**, or over** R. The zero and the identity of $R[X]$ are the zero and identity of R, respectively.

Note: The elements of R can be identified with polynomials of degree 0. I will call these polynomials **constant**. You should notice from the multiplication rule that if R is commutative, then so is $R[X]$

Theorem 2.3.3: Zero-Divisors of a Polynomial Ring

If R is a ring with no zero-divisors, then $R[X]$ has no zero-divisors and $\deg(PQ) = \deg(P) + \deg(Q)$ for non-zero $P, Q \in R[X]$.

If R is an integral domain, then so is $R[X]$

Theorem 2.3.4: Division and Remainder

Let R be an integral domain and let $P, Q \in R[X]$ with Q monic. Then there exists unique $A, B \in R[X]$ such that $P = AQ + B$ and $\deg(B) < \deg(Q)$ or $B = 0$

Definition 2.3.5: Formal definition of a function

Let R be a commutative ring and $P \in R[X]$ a polynomial. Then the polynomial P can be **evaluated** at the element $\lambda \in R$ to produce $P(\lambda)$ by replacing the powers of X in the polynomial P by the corresponding powers of λ. In this way we have a mapping

$$R[X] \to \mathrm{Maps}(R, R)$$

This is the precise mathematical description of thinking of a polynomial as a function. An element $\lambda \in R$ is a **root** of P is $P(\lambda) = 0$

Theorem 2.3.6: Roots of a Polynomial

Let R be a commutative ring, let $\lambda \in R$ and $P(X) \in R[X]$. Then λ is a root of $P(X)$ if and only if $(X - \lambda)$ divides $P(X)$

Theorem 2.3.7: Degrees of Polynomial Roots

Let R be a field, or more generally an integral domain. Then a non-zero polynomial $P \in R[X] \backslash \{0\}$ has at most $\deg(P)$ roots in R

Definition 2.3.8: Algebraically closed fields

A field F is **algebraically closed** if each non-constant polynomial $P \in F[X] \backslash F$ with coefficients in our field has a root in our field F

Example: The field of real numbers $\mathbb{R}$ is not algebraically closed. For instance, $X^2 + 1$ has no root in $\mathbb{R}$

Theorem 2.3.9: Fundamental Theorem of Algebra

The field of complex numbers $\mathbb{C}$ is algebraically closed.

Theorem 2.3.10: Linear Factors of Algebraically Closed Fields

If F is an algebraically closed field, then every non-zero polynomial $P \in F[X] \backslash \{0\}$ **decomposes into linear factors**

$$P = c(X - \lambda_1) \cdots (X - \lambda_n)$$

with $n \geq 0$, $c \in F^\times$ and $\lambda_1, \ldots, \lambda_n \in F$. This decomposition is unique up to reordering the factors

3 Determinants and Eigenvalues Redux

3.1 Symmetric Groups

Definition 3.1.1: Symmetric Groups

The group of all permutations of the set $\{1, 2, \ldots, n\}$, also known as bijections from $\{1, 2, \ldots, n\}$ to itself is denoted by $\mathfrak{S}_n$ (but i will just write S_n because icba) and called the **n-th symmetric group**. It is a group under composition and has $n!$ elements.

A **tranposition** is a permutation that swaps two elements of the set and leaves all the others unchanged.

Definition 3.1.2: Inversions of a permutation

An **inversion** of a permutation $\sigma \in S_n$ is a pair (i, j) such that $1 \leq i < j \leq n$ and $\sigma(i) > \sigma(j)$. The number of inversions of the permutation σ is called the **length of** σ and written $\ell(\sigma)$. In formulas:

$$\ell(\sigma) = |\{(i, j) : i < j \text{ but } \sigma(i) > \sigma(j)\}|$$

The **sign of** σ is defined to be the parity of the number of inversions of σ. In formulas:

$$\operatorname{sgn}(\sigma) = (-1)^{\ell(\sigma)}$$

Note: A permutation whose sign is $+1$, in other words which has even length, is called an **even permutation**

A permutation whose sign is -1, in other words which has odd length, is called an **odd permutation**
[INSERT DIAGRAM]

Theorem 3.1.3: Multiplicativity of the sign

For each $n \in \mathbb{N}$ the sign of a permutation produces a group homomorphism $\operatorname{sgn} : S_n \to \{+1, -1\}$ from the symmetric group to the two-element group of signs. In formulas:

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) \quad \forall \sigma, \tau \in S_n$$

Definition 3.1.4: Alternating Group of a Permutation

For $n \in \mathbb{N}$, the set of even permutations in S_n forms a subgroup of S_n because it is the kernel of the group homomorphism $\operatorname{sgn} : S_n \to \{+1, -1\}$. This group is the **alternating group** and is denoted A_n

3.2 Determinants

Definition 3.2.1: Determinants

Let R be a commutative ring and $n \in \mathbb{N}$. The **determinant** is a mapping $\det : \mathrm{Mat}(n; R) \to R$ from square matrices with coefficients in R to the ring R that is given by the following formula

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \mapsto \det(A) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}$$

The sum is over all permutations of n, and the coefficient $\mathrm{sgn}(\sigma)$ is the sign of the permutation σ defined above. This formula is called the **Leibniz formula**. The degenerate case $n = 0$ assigns the value 1 as the determinant of the "empty matrix"
Remark: The determinant determines whether or not a linear system of kn equations in n unknowns has a unique solution, hence the name

3.2.2 The connection between determinants and volumes

Each such linear mapping L has an "area scaling factor" $\mathrm{sc}(L)$ which I defined as the amount that L changes the area, $\mathrm{vol}(U)$, of a region U in $\mathbb{R}^2$. In other words, $\mathrm{area}(LU) = \mathrm{sc}(L)\mathrm{area}(U)$. I claim that

$$\mathrm{sc}(L) = |\det(L)|$$

To see this, I consider the properties that the mapping $\mathrm{sc} : \mathrm{Mat}(2; \mathbb{R}) \to \mathbb{R}_{\geq 0}$, defined by $L \mapsto \mathrm{sc}(L)$, must have:

1. It should be "multiplicative": $\mathrm{sc}(LM) = \mathrm{sc}(L)\mathrm{sc}(M)$
2. Dilating an axis should increase the area of a region by the amount of the dilation:

$$\mathrm{sc}(\mathrm{diag}(a, 1)) = \mathrm{sc}(\mathrm{diag}(1, a)) = |a|$$

3. A shear transformation should leave the area of a region unchanged: $\mathrm{sc}(D) = 1$ for D an upper or a lower triangular matrix with ones on the diagonal

3.2.3 The connection between determinants and orientation

The sign of the determinant of an invertible real (2×2) matrix shows whether the corresponding endomorphism of $\mathbb{R}^2$ preseves or reverses orientation. To comprehend orientation, I imagine a clock face inside the region U I'm going to apply L to: if, after applying U, the clock face is still the correct way round then L preserves orientation; if it is the wrong way around, then L reverses orientation. I think of this property as a mapping sending an invertible linear transformation $L : \mathbb{R}^2 \to \mathbb{R}^2$ to $\epsilon(L) \in \{+1, -1\}$ as follows:

$$\epsilon(L) = \begin{cases} +1 & L \text{ preserves the orientation} \\ -1 & L \text{ reverses the orientation} \end{cases}$$

Let $[a]$ denote the sign of a non-zero real number a. I claim that

$$\epsilon(L) = [\det(L)]$$

To see this, let's consider the properties that the mapping $\epsilon : GL(2;\mathbb{R}) \to \{+1, -1\}$ defined by $L \mapsto \epsilon(L)$, must have:

1. It should be "multiplicative": $\epsilon(LM) = \epsilon(L)\epsilon(M)$
2. Dilating an axis should change the orientation by the sign of the amount of the dilation:

$$\epsilon(\text{diag}(a, 1)) = \epsilon(\text{diag}(1, a)) = [a]$$

3. A shear transformation should preserve the orientation: $\epsilon(D) = 1$ for D an upper or a lower triangular matrix with ones on the diagonal

3.3 Characterising the Determinant

Determinants exist for more than just real matrices, so here is an interpretation of the determinant over arbitrary fields

Definition 3.3.1: Bilinear Forms

Let U, V, W be F-vector spaces. A **bilinear form on $U \times V$ with values in W** is a mapping $H : U \times V \to W$ which is a linear mapping in both of its entries. This means that it must satisfy the following properties for all $u_1, u_2 \in U$ and $v_1, v_2 \in V$ and all $\lambda \in F$:

$$\begin{aligned} H(u_1 + u_2, v_2) &= H(u_1, v_1) + H(u_2, v_1) \\ H(\lambda u_1, v_1) &= \lambda H(u_1, v_1) \\ H(u_1, v_2 + u_2) &= H(u_1, v_1) + H(u_2, v_1) \\ H(u_1, \lambda v_1) &= \lambda H(u_1, v_1) \end{aligned}$$

The first two conditions state that for any fixed $v \in V$ the mapping $H(-, v) : U \to W$ is linear; the final two conditions state that for any fixed $u \in U$, the mapping $H(u, -) : V \to W$ is linear. If U, V, and W are clear from the context I will simply say that H is a **bilinear form**. A bilinear form H is **symmetric** is $U = V$ and

$$H(u, v) = H(v, u) \quad \text{for all } u, v \in U$$

while it is **antisymmetric** or **alternating** if $U = V$ and

$$H(u, u) = 0 \quad \text{for all } u \in U$$

Remark: Suppose that $H : U \times U \, toW$ is an antisymmetric bilinear form on U with values in W. Then for all $u, v \in W$:

$$\begin{aligned} 0 &= H(u + v, u + v) \\ &= H(u, u + v) + H(v, u + v) \\ &= H(u, u) + H(u, v) + H(v, u) + H(v, v) \\ &= H(u, v) + H(v, u) \end{aligned}$$

Therefore, an antisymmetric form always satisfies $H(u, v) = -H(v, u)$, hence the name. On the other hand, if H is a bilinear form satisfying $H(u, v) + -H(v, u)$ for all $u, v \in U$, then taking $u = v$ gives $H(u, u) = -H(u, u)$ from which follows that $H(u, u) + H(u, u) = 0$. As long as $1_F + 1_F \neq 0_F$ I deduce that $H(u, u) = 0$ and so the form is antisymmetric. But remember that you know a field $F = \mathbb{F}_2$ in which $1_F + 1_F = 0_F$, so you do need to be careful

Definition 3.3.2: Multilinear Forms

Let $V_1, \dots, V_n, W$ be F-vector spaces. A mapping $H : V_1 \times V_2 \times \cdots \times V_n \to W$ is a **multilinear form** or just **multilinear** if for each j, the mapping $V_j \to W$ defined by $v_j \mapsto H(v_1, \dots, v_j, \dots, v_n)$, with the $v_i \in V_i$ arbitrary fixed vectors of V_i for $i \neq j$ is linear.

In the case that $n = 2$, this is exactly the definition of a bilinear mapping shown above

Definition 3.3.3: Alternating Multilinear Forms

Let V and W be F-vector spaces. A multilinear form $H : V \times \cdots \times V \to W$ is **alternating** if it vanishes on every n-tuple of elements of V that has at least two entries equal, in other words if:

$$(\exists i \neq j \text{ with } v_i = v_j) \to H(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = 0$$

In the case $n = 2$, this is exactly the definition of an alternating/antisymmetric form shown above

Remark: An alternating multilinear form H has the property

$$H(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -H(v_1, \dots, v_j, \dots, v_i, \dots, v_n)$$

for all $v_1, \dots, v_n \in V$. Combining this with [WIP] shows that for any $\sigma \in S_n$,

$$H(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = \operatorname{sgn}(\sigma) H(v_1, \dots, v_n)$$

Conversely, if the above remark holds for a multilinear form H and arbitrary $v_1, \dots, v_n \in V$, then H is alternating provided that $1_F + 1_F \neq 0_F$

Theorem 3.3.4: Characterisation of the Determinant

Let F be a field. The mapping

$$\det : \operatorname{Mat}(n; F) \to F$$

is the unique alternating multilinear form on n-tuples of column vectors with values in F that takes the value 1_F on the identity matrix