# Mathematics

Edward Wang

2025

# Contents

# Part I.

# Algebra

# 1. Group Theory

## 1.1. Groups, permutations, subgroups

**Definition 1.1.1.** A *binary operation*, also referred to as a *law of composition* on a set $S$ is a mapping from $S \times S$ to $S$. We say that a binary operation $\cdot : S \times S \to S$ is

- *associative* if $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in S$,
- *commutative* if $a \cdot b = b \cdot a$ for all $a, b, \in S$.

**Remark 1.1.1.** The $\cdot$ will usually be implicit. That is, $ab$ will denote $a \cdot b$ where $\cdot$ is a binary operation.

The following are all familiar examples of laws of composition.

**Example 1.1.1.**

1. $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defines the mapping $(x, y) \mapsto x + y$.
2. $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defines the mapping $(x, y) \mapsto xy$.
3. $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defines the mapping $(a, b) \mapsto a + b$.
4. $M_{2\times 2}(\mathbb{R}) \times M_{2\times 2}(\mathbb{R}) \to M_{2\times 2}(\mathbb{R})$ has a mapping $(A, B) \mapsto AB$ (matrix multiplication).

All of the above examples were both associative and commutative, except for the last one, which was only associative (matrix multiplication does not commute in general).

**Example 1.1.2.** Let $T$ be a set, and let $M$ denote the set of functions from $T$ to $T$. Take two elements $f$ and $g$ from $M$. Then there exists a law of composition $f \circ g$, known as function composition, defined as $(f \circ g)(t) \coloneqq f(g(t))$ for all $t \in T$. This law is associative, since $(f \circ (g \circ h))(t) = f(g(h(t))) = ((f \circ g) \circ h)(t)$.

Suppose we want to find the *product* of $n$ elements $a_1 \cdots a_n$. If the law of composition is not associative, then there are many ways to write such a

product, since the law of composition is only defined for two elements. For example, we could write the product as any of

$$(a_1(a_2a_3))a_4\cdots$$
$$(a_1a_2(a_3a_4))\cdots,$$

which could all have distinct results. However, if the law is associative, then all ways will yield the same unique product.

**Proposition 1.1.1.** *Let there be given an associative law of composition on a set $S$. Then, there exists a unique way to write the product of $n$ elements, which will temporarily be denoted as*

$$[a_1\cdots a_n].$$

*We define $[a_1\cdots a_n]$ inductively with the following properties:*

1. *The product of a single element is itself: $[a_1]=a_1$.*
2. *The product of two elements is given by the law of composition: $[a_1a_2]=a_1a_2$.*
3. *For all integers $1\leq i\leq n-1$, we have $[a_1\cdots a_n]=[a_1\cdots a_i][a_{i+1}\cdots a_n]$.*

*Proof.* We will proceed via strong induction on $n$. The base case $n=1$ and $n=2$ are trivial. Now suppose that for all $k\leq n-1$, we have already defined a product $[a_1\cdots a_k]$. We must show that $[a_1\cdots a_n]$ satisfies 3.

Take $[a_1\cdots a_n]=[a_1\cdots a_{n-1}][a_n]$. Both terms on the right hand side are unique by the hypothesis, so the left hand side must also be unique. Next, we have

$$\begin{aligned}[a_1\cdots a_n]&=[a_1\cdots a_{n-1}][a_n]\\&=\big([a_1\cdots a_j][a_{j+1}\cdots a_{n-1}]\big)[a_n],\end{aligned}$$

for all $1\leq j\leq n-2$, and by associativity, we have

$$\begin{aligned}\big([a_1\cdots a_j][a_{j+1}\cdots a_{n-1}]\big)[a_n]&=[a_1\cdots a_j]\big([a_{j+1}\cdots a_{n-1}][a_n]\big)\\&=[a_1\cdots a_j][a_{j+1}\cdots a_n],\end{aligned}$$

by 3., and we are done. □

**Definition 1.1.2.** An *identity* for a given law of composition $\cdot\colon S\times S\to S$ is an element $e\in S$ such that $ea=ae=a$ for all $a\in S$.

**Remark 1.1.2.** If the law of composition is written multiplicatively, then we will usually denote the identity element by 1. Otherwise, if it is written additively, we will usually denote it by 0.

**Example 1.1.3.** Multiplication has the identity 1, and addition has the identity 0. Matrix multiplication has the identity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Function composition has the identity element $\mathrm{id}\colon X \to X$ such that $\mathrm{id}_X(x) = x$.

**Proposition 1.1.2.** *An identity element, if it exists, is unique.*

*Proof.* Let $e$ and $e'$ both be identities. Then, $ee' = e$ but also $ee' = e'e = e'$, so $e = e'$. □

**Definition 1.1.3.** Let there be a law of composition on $S$, and suppose that it has identity 1. An element $a \in S$ is *invertible* if there exists $b \in S$ such that $ab = ba = 1$. If $a$ is invertible, we call $b$ the *inverse* of $a$ and write $a^{-1} = b$.

**Proposition 1.1.3.** *If $a$ is invertible then $a^{-1}$ is unique.*

*Proof.* Suppose $b$ and $b'$ are both inverses of $a$. Then $ab = ba = 1$ and $ab' = b'a = 1$. But then $b'ab = b' = (b'a)b = 1b = b$. Hence the inverse is unique. □

**Remark 1.1.3.** We denote the product of $a$ with itself $n$ times by $\underbrace{a \cdots a}_{n} = a^n$. By convention, $a^0$ is defined to be 1 (the identity). Finally, $a^{-n}$ is the product of $a^{-1}$ by itself $n$ times. That is, $\underbrace{a^{-1} \cdots a^{-1}}_{n} = a^{-n}$.

**Definition 1.1.4** (Group)**.** A *group* is a set $G$ with a law of composition such that

1. the law of composition is associative,
2. $G$ contains an identity element,
3. every element of $G$ is invertible.

More formally, a group is an ordered pair of a set $G$ and a binary operation $\cdot$ on $G$ that satisfies the three group axioms.

**Definition 1.1.5.** If the law of composition on a group $G$ is commutative, then $G$ is said to be an *abelian* group.

**Example 1.1.4.**

- Addition is a group over $\mathbb{R}$. That is, $(\mathbb{R}, +)$ is a group. Moreover, it is abelian.
- $(\mathbb{Z}, \times)$ is not a group, because integers do not have multiplicative inverses.
- $(M_{2\times 2}(\mathbb{R}), \cdot)$ is not a group because some matrices are not invertible.
- Take $\mathbb{R}^\times \coloneqq \mathbb{R} \setminus \{0\}$. Then $\mathbb{R}^\times$ is a group under multiplication.
- Let $\mathrm{GL}_n(\mathbb{R})$ be the set of $n \times n$ invertible matrices with real entries. Then $\mathrm{GL}_n(\mathbb{R})$ is a group under matrix multiplication. Note that it is not abelian, since matrix multiplication is not, in general, commutative.

**Definition 1.1.6.** The *order* of a group $(G, \cdot)$ is the number of elements in $G$. This is denoted by $|G|$. If $|G| < \infty$, then $G$ is a *finite* group. Otherwise, it is an *infinite* group.

**Proposition 1.1.4** (Cancellation law)**.** *Let $(G, \cdot)$ be a group, and take $a, b, c \in G$. Then, both of the following are true:*

1. *If $ab = ac$ or $ba = ca$, then $b = c$.*
2. *If $ab = a$ or $ba = a$, then $b = 1$.*

*Proof.*

1. Take $ab = ac$. Left multiplying by $a^{-1}$ gives $a^{-1}b = a^{-1}c$ so $b = c$. The other case follows identically.
2. Take $c = 1$ in part 1.

□

**Definition 1.1.7.** A *permutation* is a bijection $\sigma\colon S \to S$. The set of permutations of a set $X$ is denoted $S_X$ and called the *symmetric group* of $X$. In particular, if $X = \{1, 2, \ldots, n\}$ and $|X| = n$, we write $S_n$ and say that it is the symmetric group of degree $n$.

**Proposition 1.1.5.** *The symmetric group $S_n$ is a group under function composition. That is, $(S_n, \circ)$ is a group.*

*Proof.* We must check that function composition is closed and associative, all elements are invertible and that there exists an identity.

1. Obviously, the composition of two bijections is also a bijection. Hence $S_n$ is closed under $\circ$.
2. It is also obvious that function composition is associative (we proved this earlier).
3. Since all bijections are invertible, we know that all elements of $S_n$ have an inverse.
4. Finally, the identity function id which maps every element to itself is the identity.

Hence $(S_n, \circ)$ is a group. □

**Remark 1.1.4.** The order of $S_n$ is $|S_n| = n!$.

**Example 1.1.5.** Take $\sigma \in S_5$ defined according to the table

| $i$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $\sigma(i)$ | 2 | 3 | 1 | 5 | 4 |

We will write this as $\sigma = (123)(45)$, with each bracketed string forming a 'cycle'. In particular, 2-cycles like (45) are called *transpositions*. Note that cycle notation is not unique. In cycle notation, if an element is omitted, it is assumed that it maps to itself.

**Example 1.1.6.** Take $s, t \in S_5$, and let $s = (123)(45)$ and $t = (12)(34)$. Then $st = s \circ t = (3541)$. Similarly, $ts = t \circ s = (2453)$. Note that $st \neq ts$ so $S_n$ is not abelian.

Every permutation has an associated permutation matrix. The idea is that for every $s \in S_n$, there exists $P_s \in M_{n\times n}$ such that $P_s A$ permutes the rows of $A$ according to $s$. This is trivially constructed by applying the permutation to *columns* of the identity matrix. We have

$$(P_s)_{ij} = \begin{cases} 1 & s(j) = i \\ 0 & \text{otherwise.} \end{cases}$$

For example, consider the permutation $s = (123)(45)$. Take the standard basis vectors $\mathbf{e_1} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ and so on. We want $P_s\mathbf{e_1} = \mathbf{e_2}$, $P_s\mathbf{e_2} = \mathbf{e_3}$, $P_s\mathbf{e_3} = \mathbf{e_1}$ and

so on. By permuting the columns, we get

$$P = \begin{bmatrix} \mathbf{e_2} \mid \mathbf{e_3} \mid \mathbf{e_1} \mid \mathbf{e_5} \mid \mathbf{e_4} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

In fact, matrix multiplication by permutation matrices results in the composition of the permutations.

**Definition 1.1.8.** Let $P_s$ be the permutation matrix associated with $s \in S_n$. The *sign* of $s$ is defined to be $\operatorname{sgn}(s) = \det(P_s) = \pm 1$. A permutation is *even* if its sign is 1, and *odd* if its sign is $-1$.

**Remark 1.1.5.** Every permutation is a product of transpositions. This is equivalent to the fact that the permutation matrix is the result of a series of elementary row operations on the identity matrix.

**Definition 1.1.9** (Subgroup)**.** A subset $H$ of a group $G$ is a *subgroup* if $H$ is a group with respect to the law of composition of $G$.

**Example 1.1.7.**

1. $\mathbb{R}^\times$ is a subgroup of $\mathbb{C}^\times$ under multiplication.
2. $\{z \in \mathbb{C} : |z| = 1\}$ is a subgroup of $\mathbb{C}^\times$. This is the *circle group*.
3. $\{A \in \mathrm{GL}_n(\mathbb{R}) : \det(A) = 1\}$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$. In fact, this subgroup is so important that we give it a name, the *special linear group*, and denote it with $\mathrm{SL}_n(\mathbb{R})$.

**Remark 1.1.6.** If $G$ is a group, then it contains two obvious subgroups: $G$ itself and $\{1\}$ (the *trivial group*).

**Definition 1.1.10.** A subgroup $H$ of $G$ is a *proper* subgroup if $H \neq G$.

With this definition, the trivial subgroup is a proper subgroup of any non-trivial group.

Take a positive integer $a$. Then, the set of all multiples of $a$ is denoted by

$$a\mathbb{Z} \coloneqq \{x \in \mathbb{Z} : x = ak, \text{ where } k \in \mathbb{Z}\}.$$

**Proposition 1.1.6.** *The set $a\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ under addition.*

**Proposition 1.1.7.** *TODO*

**Theorem 1.1.1.** *Let $S$ be a subgroup of $(\mathbb{Z}, +)$. Then either $S = \{0\}$ or $S = a\mathbb{Z}$ for some positive integer $a$.*

*Proof.* Suppose that $S$ is non-trivial, and contains some element other than 0. □

Take two positive integers $a$ and $b$ and define the set

$$a\mathbb{Z} + b\mathbb{Z} \coloneqq \{ar + bs : r, s \in \mathbb{Z}\}.$$

**Proposition 1.1.8.** *The set $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ under addition.*

*Proof.* TODO □

Since $a\mathbb{Z} + b\mathbb{Z}$ is a (non-trivial) subgroup of $\mathbb{Z}$, by Theorem 1.1.1, it must be equal to some $d\mathbb{Z}$.

**Definition 1.1.11.** Let $d$ be the unique positive integer such that $a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$. We call $d$ the *greatest common divisor* of $a$ and $b$, denoted $d = \gcd(a, b)$.

**Proposition 1.1.9.** *The greatest common divisor defined in this way has the same properties as the usual definition of the greatest common divisor. That is, if $d = \gcd(a, b)$, then*

1. *$d \mid a$ and $d \mid b$,*
2. *if $e \in \mathbb{Z}$ and $e \mid a$ and $e \mid b$, then $e \mid d$,*
3. *there exists $r, s \in Z$ such that $ar + bs = d$.*

*Proof.* TODO □

**Proposition 1.1.10** (Euclidean algorithm)**.** *Let $n, d$ be natural numbers such that $n = qd + r$. Then,* $\gcd(n, d) = \gcd(d, r)$.

*Proof.* We will prove that the set of common divisors of $n$ and $d$ is the same as the set of common divisors of $d$ and $r$.

Suppose $a$ is a common divisor of $n$ and $d$, that is, $a \mid n$ and $a \mid d$. This means that $a \mid n\alpha + d\beta$ for any integers $\alpha, \beta$. Specifically, we have $a \mid n - qd = r$, so $a \mid r$. Therefore $a$ is a common divisor of $n$ and $r$.

Similarly, suppose $a$ is a common divisor of $d$ and $r$, that is, $a \mid d$ and $a \mid r$. We have $a \mid qd + r = n$, so $a \mid n$. Therefore $a$ is a common divisor of $n$ and $d$.

The set of divisors are therefore the same, so the greatest common divisor must also be the same. □

**Example 1.1.8.** We can find the greatest common divisor of two numbers using the Euclidean algorithm. For example, let $a = 154$ and $b = 62$. Since $a = 2b + 30$, we have

$$\begin{aligned} a\mathbb{Z} + b\mathbb{Z} &= (2b + 30)\mathbb{Z} + b\mathbb{Z} \\ &= b\mathbb{Z} + 30\mathbb{Z}. \end{aligned}$$

Now $b = 2 \times 30 + 2$, so

$$\begin{aligned} b\mathbb{Z} + 30\mathbb{Z} &= (2 \times 30 + 2)\mathbb{Z} + 30\mathbb{Z} \\ &= 30\mathbb{Z} + 2\mathbb{Z}. \end{aligned}$$

Now the greatest common divisor is obviously 2. Hence $d = 2$.

**Definition 1.1.12.** Two non-zero integers $a, b$ are *coprime*, or *relatively prime*, if $\gcd(a, b) = 1$. That is, $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.

**Proposition 1.1.11.** *Two non-zero integers $a$ and $b$ are coprime if and only if there exist $r, s$ such that $ar + bs = 1$.*

*Proof.* TODO □

**Proposition 1.1.12** (Euclid's lemma)**.** *Let $p$ be a prime number, and let $a, b$ be non-zero integers. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

*Proof.* TODO □

**Proposition 1.1.13.** *Let $a, b$ be non-zero integers. Then $a\mathbb{Z} \cap b\mathbb{Z}$ is a subgroup.*

*Proof.* TODO □

Hence by Theorem 1.1.1, $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ for some integer $m$.

**Definition 1.1.13.** For any two non-zero integers $a$ and $b$, the *least common multiple* of $a$ and $b$ is $m$ such that $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. We denote $m$ by $\operatorname{lcm}(a, b)$.

**Proposition 1.1.14.** *Let $a, b$ be non-zero integers and let $m = \operatorname{lcm}(a, b)$. Then,*

1. $a \mid m$ *and* $b \mid m$,
2. *if* $a \mid n$ *and* $b \mid n$, *then* $m \mid n$.

*Proof.* TODO □

**Corollary 1.1.1.** *Let* $d = \gcd(a, b)$ *and* $m = \gcd(a, b)$ *for two non-zero integers* $a, b$. *Then* $ab = dm$.

## 1.2. Cyclic groups

**Definition 1.2.1.** Let $G$ be a group and take $x \in G$. The *cyclic subgroup* of $G$ genearted by $x$ is

$$\langle x \rangle \coloneqq \{x^k : k \in \mathbb{Z}\}$$

**Proposition 1.2.1.** *Let* $G$ *be a group and take* $x \in G$. *Let* $\langle x \rangle$ *be the cyclic subgroup generated by* $x$. *Suppose* $S = \{k \in \mathbb{Z} : x^k = 1\}$. *Then,*

1. *the set* $S$ *is a subgroup of* $(\mathbb{Z}, +)$,
2. $x^r = x^s$ *if and only if* $x^{r-s} = 1$

*Proof.* TODO □

# 2. Linear Algebra

## 2.1. Vector spaces

We begin by recalling the definition of vector spaces.

**Definition 2.1.1** (Vector space)**.** Let $\mathbb{F}$ be a field. A *vector space* over $\mathbb{F}$ is a set $V$ with a binary operation $+$ and function $\cdot\colon \mathbb{F} \times V \to V$ such that

- $(V, +)$ is an abelian group with identity $\mathbf{0}$,
- $1v = v$ for all $v \in V$ (identity),
- $a(bv) = (ab)v$ for all $a, b \in \mathbb{F}$ and $v \in V$ (associativity),
- $a(u + v) = au + bv$ and $(a + b)v = av + bv$ for all $a, b \in \mathbb{F}$ and $u, v \in V$ (distributivity).

**Example 2.1.1.** Common examples of vectors spaces include

- $\mathbb{F}^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}\}$ (e.g. $\mathbb{R}^2$)
- $M_{m\times n}(\mathbb{F})$, the set of $m \times n$ matrices with entries in $\mathbb{F}$
- $P_n(\mathbb{F})$, the set of polynomials of degree $n$ with coefficients in $\mathbb{F}$
- $C(\mathbb{R}, \mathbb{R})$, the set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$
- $C^1(\mathbb{R}, \mathbb{R})$, the set of differentiable functions from $\mathbb{R}$ to $\mathbb{R}$

Linear algebra is the study of linear transformations — maps that preserve vector addition and scalar multiplication.

**Definition 2.1.2** (Linear transformation)**.** Let $V, W$ be vector spaces over $\mathbb{F}$. A *linear transformation*, or *linear map*, is a function $T\colon V \to W$ such that:

- $T(u + v) = T(u) + T(v)$ for all $u, v \in V$,
- $T(\alpha v) = \alpha T(v)$ for all $\alpha \in \mathbb{F}$, $v \in V$.

A linear transformation from $V$ to itself is a *linear operator*.

Indeed, linear transformations are a kind of homomorphism. To this end, we will let $\mathrm{Hom}(V, W)$ denote the set of linear transformations from $V$ to $W$. (This is also sometimes notated as $\mathcal{L}(V, W)$.)

**Proposition 2.1.1.** *The set of linear transformations from $V$ to $W$, $\mathrm{Hom}(V, W)$ is a vector space.*

*Proof.* We first show that linear transformations form an abelian group under multiplication. Obviously there is an additive identity, the zero map that takes every element to the zero vector. Let $S, T \in \mathrm{Hom}(V, W)$. Then define $(S + T)(v) \coloneqq S(v) + T(v)$. This is obviously a linear map. It is also not hard to verify that scalar multiplication works as it should in a vector space, and that distributivity holds. □

**Definition 2.1.3.** A linear transformation $T \colon V \to W$ is *invertible* if there exists a linear transformation $S \colon W \to V$ such that $TS = I_V$ and $ST = I_W$.

**Proposition 2.1.2.** *A linear transformation is invertible if and only if it is bijective.*

*Proof.* TODO □

**Definition 2.1.4.** A linear transformation that is bijective is an *isomorphism.*

**Proposition 2.1.3.** *Let $U, U', V, V'$ be vector spaces over $\mathbb{F}$, and suppose that $\varphi \colon U \to U'$ and $\psi \colon V \to V'$ are isomorphisms. Then the map $\Phi \colon \mathrm{Hom}(U, V) \to \mathrm{Hom}(U', V')$ where $\Phi = \psi \circ T \circ \varphi^{-1}$ is an isomorphism.*

*Proof.* We need to show that $\Psi$ is both a linear transformation and bijective. Also refer to the commutative diagram [TODO] □

We know that every linear transformation has a corresponding matrix. This is because every linear transformation is completely defined by its values on a generating (spanning) set. That is, suppose $S \subseteq V$ is a set that spans $V$. This means that every vector in $V$ is a linear combination of the vectors in $S$. Then the values that a linear transformation $T \colon V \to W$ takes for all $s \in S$ completely define it. In other words, if we know $T(s)$ for all $s \in S$ where $S$ spans $V$, then we know $T$.

**Definition 2.1.5.** A set $S \subseteq V$ is said to *span* $V$ if any $v$ in $V$ can be written as a linear combination of vectors in $S$. That is, if $S = \{s_1, s_2, \ldots, s_n\}$, then for any $v \in V$ we can write

$$v = \alpha_1 s_1 + \cdots + \alpha_n s_n$$

for scalars $\alpha_i \in \mathbb{F}$.

**Definition 2.1.6.** Let $S = \{s_1, s_2, \ldots, s_n\} \subseteq V$. Then $S$ is said to be *linearly independent* if

$$\alpha_1 s_1 + \cdots + \alpha_n s_n = \mathbf{0}$$

if and only if $\alpha_i = 0$ for all $1 \leq i \leq n$.

**Definition 2.1.7.** A *basis* for a vector space $V$ is a linearly independent set that spans $V$.

**Remark 2.1.1.** We only deal with *finite* dimensional vector spaces here, so all our bases have a finite number of elements. In addition, our definition is technically a *Hamel* basis, as there are a number of ways to define a basis.

**Proposition 2.1.4.** *Any two bases of a vector space have the same number of elements.*

*Proof.* TODO □

**Definition 2.1.8.** The *dimension* of a vector space $V$ is the number of elements in a basis of $V$, and is denoted $\dim(V)$.

Bases are a useful way to assign coordinates to vectors. In particular, if $\dim(V) = n$, then $\mathbb{F}^n$ is isomorphic to $V$, where $V$ is a vector space. The isomorphism is formed by choosing a basis of $V$.

Suppose that $V$ is a vector space and let $B$ be a basis of $V$. If $v \in V$, then we write the *coordinate vector* of $v$ with respect to $B$ as $[v]_B$ or $B^{-1}v$.

If $B = \{v_1, v_2, \ldots, v_n\}$ and $v = \sum_{i=1}^{n} \alpha_i v_i$, then we can write the column vector

$$[v]_B = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}.$$

In fact, we can define (by abuse of notation) the map $B \colon \mathbb{F}^n \to V$ where $(x_1, \ldots, x_n) \mapsto x_1 v_1 + \cdots + x_n v_n$.

Now consider a linear map $T\colon U \to V$, where $\dim U = n$ and $\dim V = m$. Let $B$ and $B'$ be bases for $U$ and $V$ respectively. Then $(B')^{-1} \circ T \circ B \in \mathrm{Hom}(\mathbb{F}^n, \mathbb{F}^m) \cong M_{m\times n}(\mathbb{F})$.

Let's see what's going on here. We basically are mapping an element of $\mathbb{F}^n$ to an element of $\mathbb{F}^m$ by the following process:

$$\mathbb{F}^n \xrightarrow{B} U \xrightarrow{T} V \xrightarrow{(B')^{-1}} F^m.$$

Moreover, this map is a linear map since it is the composition of a bunch of linear maps ($B$, $B'$ are isomorphisms), so $(B')^{-1} \circ T \circ B$ is also a linear map from $\mathbb{F}^n$ to $\mathbb{F}^m$. We also know that maps from $\mathbb{F}^n$ to $\mathbb{F}^m$ are represented as matrices. In particular, if $U = V$, then we will write $B^{-1} \circ T \circ B = [T]_B$.

**Example 2.1.2.** Let $T\colon P_2(\mathbb{F}) \to P_2(\mathbb{F})$ be the map defined by $T(p(x)) = \frac{d}{dx}p(x)$. Then,

$$\begin{aligned}\frac{d}{dx}(1) &= 0\\ \frac{d}{dx}(x) &= 1\\ \frac{d}{dx}(x^2) &= 2x\end{aligned}$$

so

$$[T]_B = \begin{bmatrix}0 & 1 & 0\\ 0 & 0 & 2\\ 0 & 0 & 0\end{bmatrix}.$$

# Part II.

# Analysis

# 3. Real Analysis

# Part III.

# Probability

# 4. Probability