# MAT 240 Algebra I

Brian Zu

2025 Fall

# Contents

## 0.1 Introduction

The course is mainly based on the book *Linear Algebra 4th edition by S.H.Friedberg*, coupled with *A Readable Introduction to Real Mathematics* by F. Su

# Chapter 1

# Week 1

## 1.1 Sets, Functions, Fields

**Definition 1.1.1: Sets**

A set is a collection of elements. If $x$ is in the set $S$, we write $x \in S$. If not, we write $x \notin S$. Two ways of defining a set:

1. Listing the objects in that set
$$S = \{1, 2, 3, 6\} = \{2, 1, 3, 6\}$$

**Note:-**

Note that the order of elements does not matter, and repeated elements are only listed once.

2. Describing or characterizing the elements of $S$
$$A = \{x : x \text{ is a positive integer dividing } 6\}$$

**Note:-**

$A = S$

**Example 1.1.1**

$$P = \{x : x \; is \; a \; prime \; nuber\}$$

- $Z$ integers
- $Q$ the rational numbers
- $R$ the real numbers

Two sets are equal if they contain the **same elements** if $S$ and $T$ and equal, we write $S = T$

**Example 1.1.2**

$$B = \{-1, 0, 1, 2, 3, 4, 5, 6, 7\}$$
$$C = \{2, 3\} = \{x : x \text{ is an integer between } 2\&3\}$$

**Definition 1.1.2: Subset**

If $S$ and $T$ are set such that all elements of $s$ are contained in $T$, we say that $S$ is a subset of $T$ and we write $S \subset T$
If $S$ is a subset of $T$ and $S \neq T$, we write $S \subsetneq T$ and say that $S$ is a proper subset of $T$

**Definition 1.1.3: Empty Set**

The empty set is the set containing no elements, denoted by $\emptyset$ or $\{\}$. If $S$ and $T$ are sets. $S \cup T = \{x : x \in S \text{ or } x \in T\}$ is called the **union** of $S$ and $T$. $S \cap T = \{x : x \in S \text{ and } x \in T\}$ is called the intersection of $S$ and $T$.

**Example 1.1.3**

$$N = \{x \in \mathbb{Z} : x > 0\} = \{1, 2, 3, 4...\}$$

Let $-N = \{x \in \mathbb{Z} : x < 0\} = \{-1, -2, -3, -4...\}$ then $N \cap -N = \emptyset$ and $N \cup -N = \{x \in \mathbb{Z} : x \neq 0\}$. If we have a list $S_1, ..., S_k$ of sets, we can write

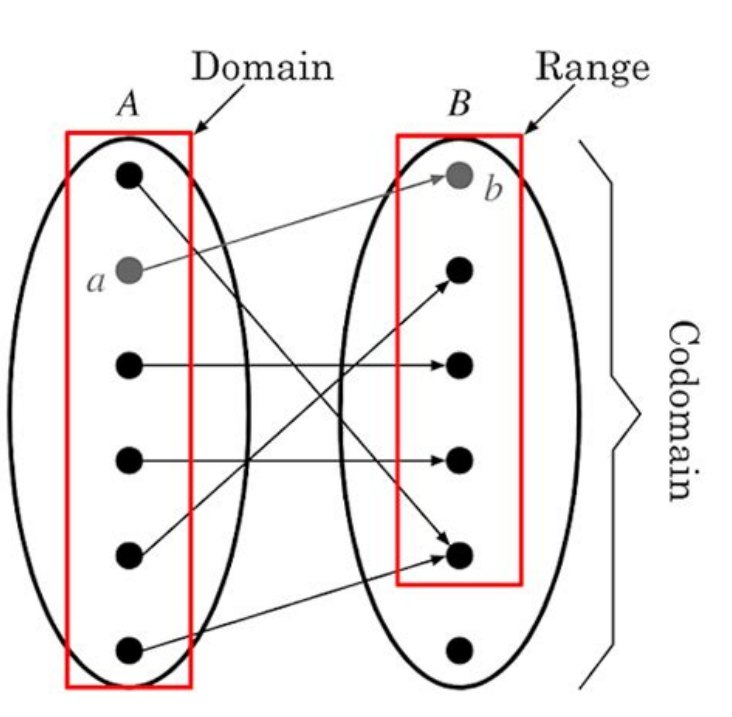
$$\bigcup_{i=1}^{k} S_i = \{x : x \in S_i \text{ for at least one of the } S_i, i = 1, .., k\}$$

$$\bigcap_{i=1}^{k} S_i = \{x : x \in S_i \text{ for all of the } S_i, i = 1, .., k\}.$$

**Definition 1.1.4: Function**

Consider two sets $A$ and $B$, and suppose that with each element x of $A$ there is associated, in some manner, an element of $B$, which denoted by $f(x)$. Then $f$ is said to be a function from $A$ to $B$, denoted by $f : A \to B$.

- The set $A$ is called the **domain** of $f$
- The set $B$ is called the **codomain** of $f$
- The elements $f(x)$ are called the **values** of $f$
- The set of all values of $f$ is called the **range** of $f$




If $E \subset A$, $f(E)$ is defined to be the set of all elements $f(x)$, for $x \in E$. We call $f(E)$ the **image** of $E$ under $f$.
If $E \subset B$, $f^{-1}(E)$ denotes the set of all $x \in A$ such that $f(x) \in E$. We call $f^{-1}(E)$ the **preimage** of $E$ under $f$.

**Definition 1.1.5: Equality of functions**

Two functions $f, g : S \to T$ are equal if $f(x) = g(x)$ for all $x \in S$

**Example 1.1.4**

For example, let $S = \{x \in \mathbb{R} : |x| \geqslant 1\}$ $f : S \to \mathbb{R}$ is the function s.t. $f(x) = \frac{1}{x^2}$. Then

- domain is $S$
- codomain is $\mathbb{R}$
- range is $\{x \in \mathbb{R} : 0 < x < 1\} \subset \mathbb{R}$

**Definition 1.1.6: Injective, surjective, and bijective**

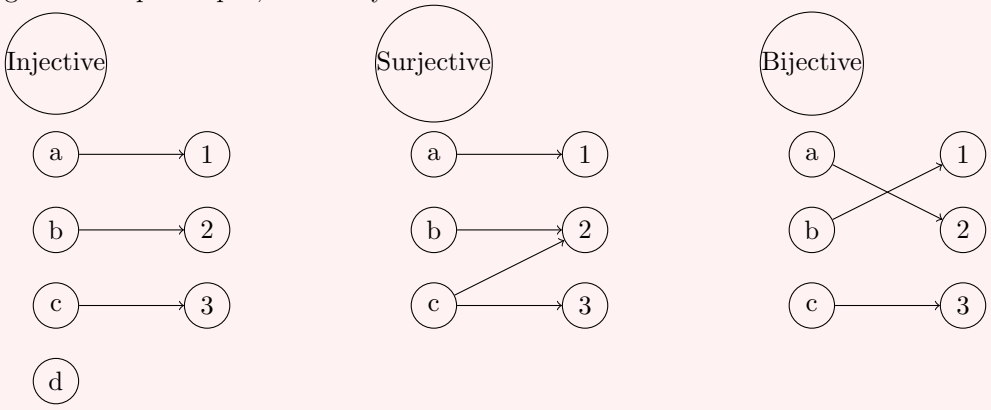
If every element is the range of $f$ has a unique preimage, we say that $f$ is **injective** or one-to-one. In notation:

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

A counter example would be $f(x) = x^2$. If every element in the codomain is in the image, we say that $f$ is **surjective** (onto). In other words, the range equals the codomain. In notation:

$$\forall y \in B, \exists\ x \in A \text{ such that } f(x) = y$$

If $f$ is surjective and injective, we say that $F$ is bijective or a bijection. It's perfect pairing — each input gives a unique output, and every element of the codomain is used.




If $f : S \to T$ and $U \subset S$ the **restriction** of $f$ to $U$ is denoted $f|_U : U \to T$. $f|_U(u) = f(u)$ for all $u \in U$

**Example 1.1.5**

Let $f : \mathbf{Z} \to \mathbf{N}$ be defined by $f(x) = |x| + 1$. Then $f$ is surjective but not injective. The function $f|_{\mathbf{N}}$ is injective but not surjective because 1 is in it's range but doesn't have a preimage. Let $\mathbf{Z}_{\geqslant 0} = \{x \in \mathbf{Z} : x \geqslant 0\}$. Then $f|_{z \geqslant 0}$ is both injective and surjective, hence a bijection.

**Example 1.1.6** (Composite functions)

let $S, T, U$ as sets,

$$f : S \to T, g : T \to U$$

The composite $g \circ f : S \to U$.

**Note:-**

Note that given $S, T$ and $f, g : S \to S$. $f \circ g$ doesn't necessarily equal to $g \circ f$. For example $f(x) = x + 1$ and $g(x) = 2x$.

**Example 1.1.7**

Exercise: check that $f, g$ is invertible and $s \in S$, $f^{-1}(s)$ .
Is $f : \mathbb{R} \to \mathbb{R}$ invertible?
$f(x) = 3x + 1$ has inverse $g(x) = (x - 1)/3$ Is $f : \mathbb{Z} \to \mathbb{Z}$ invertible?
For $f(z) = 3z + 1$, the inverse $g(x) = (x - 1)/3$ will make some of the output not integers. For example $f(g(2))$.

**Question 1**

Exercise: how to prove a function is invertible if it's bijective?

**Note:-**

The definition of field and properties are noted down in note for baby Rudin, thus disregard.

**Definition 1.1.7: Equivalence relations**

- F(1) **Commutativity** - $a+b=b+a$ and $a\cdot b=b\cdot a$
- F(2) **Associativity** - $(a+b)+c=a+(b+c)$ and $(a\cdot b)\cdot c=a\cdot(b\cdot c)$
- F(3) **Existence of Identity Elements** - There exists elements $0\in F$ and $1\in F$ such that $0+a=a$ and $1\cdot a=a$. 0 is called the **additive identity** and 1 is the **multiplicative identity**. Note that $0\neq 1$
- F(4) **Existence of Inverses** - For each $a\in F$ there exists $b\in F$ and nonzero $c\in F$ such that $a+b=0$ and $a\cdot c=1$
- F(5) **Distributivity** - $a\cdot(b+c)=ab+ac$

**Definition 1.1.8: Equivalence relations**

Let $S$ be a set. A relation on $S$ is a subset $R\subset S\times S$. We say a pair $(x,y)\in S\times S$ satisfies the notation if $(x,y)\in\mathbb{R}$. We typically denote the relation $\sim$ and while $x\sim y$ if $(x,y)\in R$. For example $\sim$ could be $=$

**Definition 1.1.9**

A relation on $S$ is an equivalence relation if it satisfies the following 3 properties $\forall x,t\in S$

- $s\sim s$
- $s\sim t\Rightarrow t\sim s$
- $s\sim t$ and $t\sim u\Rightarrow s\sim u$

**Definition 1.1.10**

If $(s,\sim)$ is a set equipped with a equivalence relation and $t\in S$, let $C_t=\{s\in S:s\sim t\}$

**Theorem 1.1.1**

Let $(s,\sim)$ is a set equipped with an equivalence relation, then $\exists\ T\subset S$ such that

- $S=\bigcup_{t\in T}C_t$
- $C_t\cap C_{t'}=\emptyset$ if $t\neq t'$

We call $T$ a set of representation for $\sim$

# Chapter 2

# Week 2

## 2.1 Modular Arithmetic

**Definition 2.1.1**

Let $m \in \mathbb{N}$. Let $a, b \in \mathbb{Z}$. We say that $a$ is congruent to $b \pmod{m}$, denoted $a \equiv b \pmod{m}$. If $m|(b-a)$.

**Example 2.1.1**

Let $a = 3$, $b = 45$. Then $a \equiv b \mod 2$ and $\mod 3$

**Lemma 2.1.1** $a \equiv b(m)$ if and only if (iff) there exists $k \in \mathbb{Z}$ such that $a = b + km$.

***Proof:*** Suppose $a \equiv b(m)$ then by definition $m|b-a$. This means that $b-a$ is a multiple of $m$, so it can be written as $b - a = mk$ for some $k \in \mathbb{Z}$. Rearranging, we have $b = a + mk$ or $a = b + (-k)m$. $-k$ is our desired multiple.
From another direction, suppose that $a = b + mk$ then $b - a = -mk$ which is divisible by m. By definition, $a \equiv b(m)$. 😄

**Theorem 2.1.1** Let $m \in \mathbb{N}$. For each $a \in \mathbb{Z}$, there exists a unique $r \in \{0, \dots, m-1\}$ such that $a \equiv r \pmod{m}$.

***Proof:*** We will prove that there exist unique integers $k, r$ such that $a = km + r$ with $0 \leqslant r < m$. By a previous lemma, this implies $a \equiv r \pmod{m}$.
**Existence.** Consider all multiples of $m$, $\{0, \pm m, \pm 2m, \dots\}$, which cover the real line by the Archimedean property. Since $a$ is an integer, there exists $k$ such that

$$km \leqslant a < (k+1)m.$$

Subtracting $km$ gives $0 \leqslant a - km < m$. Define $r = a - km$, then $a = km + r$ with $0 \leqslant r < m$.
**Uniqueness.** Suppose $a = km + r = k'm + r'$ with $0 \leqslant r, r' < m$. Then $r - r' = (k' - k)m$, so $r - r'$ is a multiple of $m$. On the other hand, since both $r$ and $r'$ lie in $[0, m)$, their difference satisfies

$$-m < r - r' < m.$$

The only multiple of $m$ in this range is 0, hence $r - r' = 0 \implies r = r'$ and then $k = k'$.

😄

For the equivalence relation of congruence modulo $m$, we have

$$\mathbb{Z} = C_0 \cup C_1 \cup \cdots \cup C_{m-1},$$

where $C_r = \{a \in \mathbb{Z} : a \equiv r \pmod{m}\}$. We call $\{0, \dots, m-1\}$ the *standard representatives*.

**Theorem 2.1.2** If $a \equiv b(m)$ and $c \equiv d(m)$, then $a + c \equiv b + d(m)$, $a \cdot c \equiv b \cdot d(m)$

***Proof:*** By lemma, $a = b + km$, $c = d + k'm$.

$$a + c = b + km + d + k'm = b + d + (k + k')m \equiv b + d(m)$$

$$a \cdot c = (b + km)(d + k'm) = bd + kmd + k'mb + kk'm^2 = bd + m(kd + k'b + kk'm) \equiv bd(m)$$

😄

**Definition 2.1.2**

The integers modulo $m$, denoted $\mathbb{Z}/m\mathbb{Z}$ is the set of equivalence classes mod $m$. We will denote it $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \bar{m-1}\}$. Thanks to the last theorem, $\mathbb{Z}/m\mathbb{Z}$ is equipped with addition and multiplication. Regular reputation in $\mathbb{Z}+$ remainder after division by $m$.

**Definition 2.1.3**

A prime number is $p \in \mathbb{N}, p > 1$, and s.t. For all $x, y \in \mathbb{Z}$, if $p \nmid x, p \nmid y \Rightarrow p \nmid xy$

**Theorem 2.1.3** $\mathbb{Z}/m\mathbb{Z}$ is a field iff $m$ is a prime

***Proof:*** Suppose that $m$ is **not** a prime. Then $\exists\, 0 < r, s < m$, such that $m = r \cdot s$. Assume for contradiction that there $\exists\, t, u$ s.t. $r \cdot t = 1, s \cdot u = 1$ which are the existence of multiplicative inverses. Then in $\mathbb{Z}/m\mathbb{Z}$. $1 = 1 \cdot 1 = s \cdot u \cdot r \cdot t = u \cdot t \cdot r \cdot s = u \cdot t \cdot 0 = 0$. Since $1 \neq 0$, this is a contradiction. So $m$ is not prime $\Rightarrow \mathbb{Z}/m\mathbb{Z}$ is not a field.
Assuming that $m$ is **prime**.

**Lemma 2.1.2** if $p$ is prime and $p \nmid x, p \nmid y, then p \nmid xy$

**Claim 2.1.1** Let $x \in \mathbb{Z}/m\mathbb{Z}$ and $m$ is prime then if $x \neq 0$

***Proof:*** Let $a, b \in \mathbb{Z}$, suppose $a \neq b(m)$, then $m \nmid a - b$. Fix a representative of $x \in \mathbb{Z}$ call it $\tilde{x}$. Since $x \neq 0, m \nmid \tilde{x}$. Since $m$ is prime, $m \nmid \tilde{x}(a - b)$, so $\tilde{x}a \not\equiv \tilde{x}b \mod m$. I.e $xa \neq xb \in \mathbb{Z}/m\mathbb{Z}$. This proves the claim. 😄

We know multiplication by $x$ is **injective**. By HW1, Q1(b) is also **surjective**. In other words, $\forall s \in \mathbb{Z}/m\mathbb{Z}, \exists\, y$ s.t. $xy = s$. In particular, $\exists\, y$ s.t. $xy = 1$. It follows that any element $x \neq 0$ has a multiplicative inverse, so if $m$ is prime, $\mathbb{Z}/m\mathbb{Z}$ is a field. Upshot: $\mathbb{Z}/p\mathbb{Z}$ is a field for all prime. We will denote it $\mathbb{F}_p$ 😄

Once proved that multiplicative and additive inverses of $a$ are unique in a field, we'll denote them respectively by $a^{-1}$ and $-a$.

# Chapter 3

# Week 3

## 3.1 Vector Space

**Definition 3.1.1: Vector Space**

Let $\mathbb{F}$ be a field. A vector space over $\mathbb{F}$ is a set $V$ equipped with two operations:

1. $+ : V \times V \to V$, $(v, w) \mapsto v + w$
2. $\mathbb{F} \times V \to V$, $(a, v) \mapsto av$, where $a$ is a scalar product of $v$.

Elements of $\mathbb{F}$ will be called scalars. Satisfying that for all $x, y, z \in V$, $a, b \in \mathbb{F}$:

1. **Commutativity of addition** $x + y = y + x$
2. **Associativity** $(x + y) + z = x + (y + z)$
3. **Additive identity** $\exists\ 0 \in V$ s.t. $0 + x = x\ \forall x \in V$
4. **Inverses** $\forall x \in V, \exists\ y$ s.t $x + y = 0$
5. **Multiplicative identity** $1x = x$
6. **Associativity of multiplication** $a(bx) = (ab)x$
7. **Distributivity of scalar multiplication over vector addition** $a(x + y) = ax + ay$
8. **Distributivity of scalar addition over scalar multiplication**$(a + b)x = ax + bx$

**Example 3.1.1**

$$\mathbb{F}^n = \{(a_1, a_2, ..., a_n) : a_i \in \mathbb{F}\ 1 \leqslant i \leqslant n\}$$

$a_i$ is the ith coordinate of $(a_1, ..., a_n)$

$$(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n)$$

$$c \in \mathbb{F},\ c(a_1, ..., a_n) = (ca_1, ..., ca_n)$$

**Example 3.1.2**

Define: An $m \times n$ matrix with entries in $\mathbb{F}$ is an array of elements of $\mathbb{F}$ with $m$ rows and $n$ columns.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

**Example 3.1.3**

Let $S$ be a non empty set. Let $\mathcal{F}(S, F)$ be the set of all functions $f : S \to F$.

$$\mathcal{F}(S, F) = \{f : S \to F\}$$

**Definition 3.1.2: Properties of vector space**

Let $V$ be a vector space over $\mathbb{F}$. Then

- If $x, y, z \in V$ and $x + z = y + z$ then $x = y$
- The vector $0 \in V$ is unique
- Let $x \in V$. The vector $y$ s.t. $x + y = 0$ is unique, call it $-x$.

These properties could be derived from the axioms.

**Theorem 3.1.1**

Let $V$ be a vector space over $\mathbb{F}$. Then

1. $0v = 0 \ \forall v \in V$
2. $(-a)v = -(av) = a(-v) \ \forall a \in \mathbb{F}, v \in V$
3. $0a = 0$

**Note:-**

Note that the proofs are in notes for baby Rudin

***Proof:*** 1.

$$0v = (0 + 0)v = 0v + 0v$$

By the cancellation property, $0v$ on both sides can be canceled, so $0 = 0v$
2.

$$(-a)v + av = v(-a + a) = 0v = 0$$

$$\Rightarrow (-a)v = av$$

By doing it the other way round, we get $av = a(-v)$
3.

$$0a + 0a = (0 + 0)a = 0a$$

Since given $x + y = x \Rightarrow y = 0$, $0a = 0$ 😄

**Definition 3.1.3: x-y**

Now we can define $x - y$ by $x + (-y)$

**Definition 3.1.4: Subspaces**

Let $V$ be a vector space over $\mathbb{F}$. We say that $W \subset V$ is a **subspace** of $V$ if it is a vector space over $\mathbb{F}$ under the restriction of the operations of $V$.
Since the operations on $V$ satisfy the properties above, it is only needed to check a few things.

**Theorem 3.1.2**

Let $V$ be a vector space. Then $W \subset V$ is a subspace **iff** the following hold.

1. $W \neq \emptyset$
2. $\forall x, y \in W,\ x + y \in W$ (closed under addition)
3. $c \in \mathbb{F},\ x \in W,\ \Rightarrow cx \in W$ (closed under scalar multiplication)

***Proof:*** (Direction $\Leftarrow$) Assume that $W$ satisfies (2) and (3). Then the operations $+$ and $\cdot$ on $W$ are well-defined.
Axioms 1,2,5,6,7,8 all automatically hold since the operation on $W$ are defined from those on $V$ (inherited from). In other words, **additive identity and inverses** are the axioms to be checked.
**Additive identity** By (1) $\exists w \in W$. Then $0w = 0$ so $W$ has a 0.
**Inverses** Let $w \in W$. Then $(-1)w \in W$ by (3).

$$(-1)w + w = (-1 + 1)w = 0w = 0$$

So $(-1)w$ is the additive inverse of $w$ and is contained in $W$.

(Direction $\Rightarrow$) Suppose $W$ is a subspace. Then $0 \in W$ and by definition $\forall x, y \in W,\ x + y \in W$ and $\forall c \in \mathbb{F}$ and $x \in W$, $cx \in W$. 😄

**Corollary 3.1.1**

If $W \subset V$ is a subspace, the $0w = 0v$ and in particular $0v \in W$.

**Example 3.1.4**

$$\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$$
$$W = (x, x) : x \in \mathbb{R}$$

**Theorem 3.1.3**

The intersection of two subspaces is a subspace.

***Proof:*** Let $W_1, W_2$ be subspace of $V$

- $0 \in W_1 \cap W_2$
- If $x, y \in W_1 \cap W_2$ then

$$x + y \in W_1 \quad \text{since } W_1 \text{ is a subspace}$$
$$x + y \in W_2 \quad \text{since } W_2 \text{ is a subspace}$$
$$\Rightarrow x + y \in W_1 \cap W_2.$$

- if $x \in W1_{\cap}W_2,\ c \in \mathbb{F}$

$$cx \in W1 \text{ since } W_1 \text{ is a subspace}$$

$$cx \in W_2 \text{ since } W_2 \text{ is a subspace}$$
$$\Rightarrow cx \in W_1 \cap W_2 \Rightarrow W_1 \cap W_2 \text{ is a field.}$$

😄

## 3.2 Linear combination

**Definition 3.2.1**

Let $V$ be a vector space and $S \subseteq V, S \neq \emptyset$. A vector $v \in V$ is a linear combination of elements of $S$ is there exists $u_1, ..., u_n \in S, d_1, ...d_n \in F$ such that $v = a_1u_1 + ... + a_nu_n$. We say that $v$ is a linear combination of $u_1, ...u_n$.The $a$ are called the coefficients.

**Example 3.2.1**

Let $V = P(Q) = \{a_1x, ..., a_nx^n : a_x \in \mathbb{Q}\}$ be a vector space. Then $3x^2 + 1$ is a linear combination of $x$ and 1. The coefficients are $3, 1$.

## 3.3 Span

**Definition 3.3.1**

Let $S$ be a non empty set be a subset of $V$. The span of $S$, denoted span$(S)$ is the set of all linear combinations of elements of $S$. If $span(S) = V$, we say that $S$ spans $V$.

**Example 3.3.1**

Let $V = \mathbb{R}^3$ what's the span for $(1, 0, 1), (0, 0, 3)$

$$a, 0, c, a, c \in \mathbb{R}$$

**Theorem 3.3.1**

The span of any $S \subset V$ is a subspace $W$ such that $S \subset W$. Moreover, any subspace containing $S$ will also contain $W$.

***Proof:*** We will check the three properties of subspace:

- $span(S)$ is not empty by definition.
- If $V = \sum_{i=1}^{n} a_ju_j$, $w = \sum_{j=1}^{m} c_ju_j$ for $u_i, u_j \in S$, then $u + w = \sum_{i=1}^{n} a_iu_i + \sum_{j=1}^{m} c_ju_j$ which is a linear combination of elements of $S$.
- If $c \in F$ and $v = \sum_{i=1}^{n} a_iu_i$ with $u_i \in S$, then $cv = \sum_{i=1}^{n} ca_iu_i$ which is a linear combination of elements of $S$ so $cv \in span(s))$. $S \subset S$

😄

## 3.4 Linear Independence/Dependence

**Definition 3.4.1: Linear relation**

Let $V$ be a vector space over $\mathbb{F}$. A subset $S \subset V$ is linearly dependent if there exists $s_1, ..., s_n \in S$ and $c_1, ..., c_n \in \mathbb{F}$, **not all zero** such that

$$c_1 s_1 + ... + c_n s_n = 0$$

We call such an expression a **linear relation**. We can always do this with $c_1 = c_2 = ... = c_n = 0$. This is called the **trivial linear relation**.

**Definition 3.4.2: Linear Independence**

A list $v_1, ..., v_m$ of vectors in $V$ is **linearly independent** if the only choice of $a_1, ..., a_m \in \mathbb{F}$ that makes $a_1 v_1 + ... + a_m v_m = 0$ is $a_1 = ... = a_m = 0$. In other words, it's linearly independent if there is no nontrivial linear relation among two vectors.

**Theorem 3.4.1**

Let $S_1 \subset S_2 \subset V$. If $S_1$ is linearly dependent, then $S_2$ is linearly dependent.

***Proof:*** This is in exercise 😊

**Corollary 3.4.1**

Let $S_1 \subset S_2 \subset V$. If $S_2$ is linearly independent, then $S_1$ is linearly independent.

**Theorem 3.4.2**

Let $S \subset V$ be linearly independent, and let $v \in V \setminus S$. Then $S \cup \{v\}$ is linearly independent $\iff$ $v \notin span(S)$.

***Proof:*** ($\Rightarrow$) Suppose $S \cup \{v\}$ is linearly independent. Assume for contradiction that $v \in span(S)$. Then there exist scalars $c_1, \ldots, c_n \in \mathbb{F}$ and $s_1, \ldots, s_n \in S$ such that

$$v = \sum_{i=1}^{n} c_i s_i.$$

Rearranging gives

$$1 \cdot v + \sum_{i=1}^{n} (-c_i) s_i = 0.$$

This is a nontrivial linear relation among elements of $S \cup \{v\}$, contradicting linear independence. Hence $v \notin span(S)$.

($\Leftarrow$) Suppose $v \notin span(S)$. We show $S \cup \{v\}$ is linearly independent. Consider a linear relation

$$av + \sum_{i=1}^{n} c_i s_i = 0$$

with $s_i \in S$, $a, c_i \in \mathbb{F}$. If $a = 0$, then we have $\sum_{i=1}^{n} c_i s_i = 0$. Since $S$ is linearly independent, this implies all $c_i = 0$, so the relation is trivial.
If $a \neq 0$, then we can solve for $v$:

$$v = \sum_{i=1}^{n} \left(-\frac{c_i}{a}\right) s_i,$$

which shows $v \in span(S)$, a contradiction. Hence the case $a \neq 0$ cannot occur, so the only possible relation is trivial.
Therefore $S \cup \{v\}$ is linearly independent. 😊

## 3.5 Bases

**Definition 3.5.1**

A basis $b$ for a vector space $V$ is a subset $b \subset V$ such that:

1. $B$ is linearly independent
2. $B$ spans $V$

If $b$ is a basis for $V$, we say that the vectors in $b$ form a basis of $V$.

**Theorem 3.5.1**

Let $V$ be a vector space, and $u_1, \ldots, u_n$ be distinct vectors in $V$. Then $b = \{u_1, \ldots, u_n\}$ is a basis of $V$ if and only if each $v \in V$ can be written uniquely as a linear combination of the vectors in $b$, i.e.

$$v = c_1 u_1 + \cdots + c_n u_n$$

for unique scalars $c_1, \ldots, c_n$.

***Proof:*** ($\Rightarrow$) Suppose $b$ is a basis of $V$.
Since $b$ spans $V$, every $v \in V$ can be written as

$$v = c_1 u_1 + \cdots + c_n u_n$$

for some scalars $c_1, \ldots, c_n$. This proves *existence*.

For *uniqueness*, suppose

$$v = c_1 u_1 + \cdots + c_n u_n = d_1 u_1 + \cdots + d_n u_n.$$

Subtracting, we obtain

$$0 = (c_1 - d_1)u_1 + \cdots + (c_n - d_n)u_n.$$

Since $b$ is linearly independent, each coefficient must vanish, so $c_i = d_i$ for all $i$. Thus the representation is unique.

($\Leftarrow$) Conversely, assume that every $v \in V$ can be written uniquely as a linear combination of the vectors in $b$.
Since every vector has such a representation, $b$ spans $V$.

To prove linear independence, suppose

$$0 = c_1 u_1 + \cdots + c_n u_n.$$

But also

$$0 = 0 \cdot u_1 + \cdots + 0 \cdot u_n.$$

By uniqueness of representation, we must have $c_i = 0$ for all $i$. If there are some other nontrivial linear relation such that $0 = c_1 u_1 + ... + c_n u_n$, where not all $c_i = 0$, then it contradicts with the uniqueness assumption. Thus $b$ is linearly independent.

Therefore $b$ is a basis of $V$. 😊

**Theorem 3.5.2**

If $V$ is a vector space with a finite spanning set, then $V$ has a finite basis.

***Proof:*** Let $S$ be a finite spanning set of $V$. Our goal is to reduce $S$ step by step until we obtain a basis.

**Step 1: Check if $S$ is linearly independent.**
If $S$ is already linearly independent, then $S$ itself is a finite basis of $V$, and we are done.

**Step 2: Remove one redundant vector if $S$ is dependent.**
Otherwise, $S$ is linearly dependent. Thus there exist distinct vectors $v_1, \ldots, v_n \in S$ and scalars $a_1, \ldots, a_n \in \mathbb{F}$, not all zero, such that

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = 0.$$

Choose an index $i$ with $a_i \neq 0$. Then we can solve for $v_i$:

$$v_i = (-a_i)^{-1} \sum_{k \neq i} a_k v_k.$$

This shows that $v_i$ is a linear combination of the other vectors in $S$.

**Step 3: Show that the span does not change.**
Let $S' = S \setminus \{v_i\}$. We claim that

$$span(S) = span(S').$$

Indeed, since $S' \subseteq S$, it follows immediately that $span(S') \subseteq span(S)$. Conversely, take any $u \in span(S)$. Then

$$u = cv_i + \sum_{j=1}^{r} c_j u_j, \quad \text{for some } u_j \in S.$$

Substituting the expression for $v_i$ in terms of the other vectors, we obtain

$$u = c(-a_i)^{-1} \sum_{k \neq i} a_k v_k + \sum_{j=1}^{r} c_j u_j,$$

which is a linear combination of elements of $S'$. Thus $u \in span(S')$. Since $u \in span(S)$ was arbitrary, we conclude $span(S) \subseteq span(S')$. Therefore $span(S) = span(S')$.

**Step 4: Repeat the process.**
We have shown how to remove one redundant vector while preserving the span. If $S'$ is linearly independent, then $S'$ is a basis and we are finished. If $S'$ is still dependent, we can repeat the process, removing one vector at a time while keeping the same span.

**Step 5: Termination.**
Since $S$ is finite, this process must terminate after finitely many steps. The result is a subset $B \subseteq S$ which is finite, linearly independent, and still spans $V$. Thus $B$ is a finite basis of $V$.

**Special case.** If $V = \{0\}$, then the empty set $\varnothing$ is by convention a basis, and it is finite. 😊

**Theorem 3.5.3**

Suppose $V$ has a spanning set $G$ consisting of $n$ elements. Let $L \subset V$ be finite, linearly independent, with $m$ elements. Then:

1. $m \leqslant n$.
2. There exists a subset $H \subset G$ of size $n - m$ such that $L \cup H$ spans $V$.

***Proof:*** We argue by induction on $m = |L|$.

**Base case:** If $m = 0$, then $L = \emptyset$. Clearly $0 \leqslant n$, and choosing $H = G$ (of size $n$) gives $L \cup H = G$, which spans $V$.

**Inductive step:** Assume the result holds for all linearly independent sets of size $m$. Now let $L = \{v_1, \ldots, v_{m+1}\}$ be linearly independent. Then $\{v_1, \ldots, v_m\}$ is linearly independent, so by the inductive hypothesis, there exist $u_1, \ldots, u_{n-m} \in G$ such that

$$\{v_1, \ldots, v_m\} \cup \{u_1, \ldots, u_{n-m}\}$$

spans $V$.

In particular, $v_{m+1}$ can be expressed as

$$v_{m+1} = a_1 v_1 + \cdots + a_m v_m + b_1 u_1 + \cdots + b_{n-m} u_{n-m}.$$

Since $L$ is linearly independent, not all $b_j$ can vanish. Without loss of generality, suppose $b_1 \neq 0$. Then we may solve for $u_1$:

$$u_1 = b_1^{-1}\Big(v_{m+1} - (a_1 v_1 + \cdots + a_m v_m + b_2 u_2 + \cdots + b_{n-m} u_{n-m})\Big).$$

Hence $u_1 \in span\big(\{v_1, \ldots, v_{m+1}, u_2, \ldots, u_{n-m}\}\big)$.

It follows that

$$V = span\big(\{v_1, \ldots, v_m, u_1, \ldots, u_{n-m}\}\big) = span\big(\{v_1, \ldots, v_{m+1}, u_2, \ldots, u_{n-m}\}\big).$$

Therefore, if we let $H = \{u_2, \ldots, u_{n-m}\}$, which has size $n - (m+1)$, we obtain $L \cup H$ as a spanning set.

Thus the theorem holds for $m + 1$. By induction, it holds for all $m$. 😄

> **Corollary 3.5.1**
>
> If $V$ has a finite basis, then all bases of $V$ are finite and have the same cardinality.

***Proof:*** Let $B, B'$ be two bases of $V$. Since $B'$ spans $V$ and $B$ is linearly independent, the theorem gives $|B| \leqslant |B'|$. Reversing the roles gives $|B'| \leqslant |B|$. Hence $|B| = |B'|$.
Finally, if $V$ had one finite basis $B$ and one infinite basis $A$, then picking $|B| + 1$ elements of $A$ would give a linearly independent set larger than $B$, contradicting the theorem. Thus all bases have the same finite cardinality, called the dimension of $V$. 😄

# Chapter 4

# Tutorial

## 4.1 Week 2 tutorial

**Question 1: Problem 1. $\mathbb{Q}$ adjoin $\sqrt{3}$**

1. Prove that the following set, endowed with the usual operations is a field:

$$\mathbb{Q}[3] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$$

2. Consider the map $\varphi(a + b\sqrt{3}) = a - b\sqrt{3}$. Prove that it is a field isomorphism (i.e. $\varphi(z \cdot z') = \varphi(z) \cdot \varphi(z') \quad \varphi(z + z') = \varphi(z) + \varphi(z')$)

3. Prove that $\mathbb{Q}[3]$ is the smallest number field to contain both $\mathbb{Q}$ and $\sqrt{3}$.

4. The above means, that $\mathbb{Q}[3]$ is the "smallest" field to extend the rational numbers to contain the roots of the equation $x^2 - 3 = 0$. What does this make the complex numbers?

### 4.1.1 (i) $\mathbb{Q}^{\sqrt{3}}$ is a field

**Definition 4.1.1: Definition of $\mathbb{Q}^{\sqrt{3}}$**

$$\mathbb{Q}^{\sqrt{3}} := \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$$

with the "usual" operations

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3}, \qquad (a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}.$$

**Example 4.1.1** (Proof that $\mathbb{Q}^{\sqrt{3}}$ is a field)

***Proof:*** • **Closure.** The formulas above show that a sum or a product of two elements again has rational coefficients, hence lies in $\mathbb{Q}^{\sqrt{3}}$.

- **Additive identity and inverses.**

$$0 = 0 + 0\sqrt{3} \in \mathbb{Q}^{\sqrt{3}}, \qquad -(a + b\sqrt{3}) = (-a) + (-b)\sqrt{3} \in \mathbb{Q}^{\sqrt{3}}.$$

- **Multiplicative identity.**

$$1 = 1 + 0\sqrt{3} \in \mathbb{Q}^{\sqrt{3}}.$$

- **Non-zero multiplicative inverses.** Let $a + b\sqrt{3} \neq 0$. Then $a^2 - 3b^2 \neq 0$ (otherwise $(a/b)^2 = 3$ would give a rational root of $x^2 - 3$). Hence

$$(a + b\sqrt{3})^{-1} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} \in \mathbb{Q}^{\sqrt{3}},$$

because $(a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2$.

- **Associativity, commutativity, distributivity.** All follow from the corresponding properties of $\mathbb{R}$.

😄

### 4.1.2 (ii) $\varphi(a + b\sqrt{3}) = a - b\sqrt{3}$ is a field isomorphism

**Example 4.1.2** (Field automorphism $\varphi$)

***Proof:*** Let $\varphi : \mathbb{Q}^{\sqrt{3}} \to \mathbb{Q}^{\sqrt{3}}$ be $\varphi(a + b\sqrt{3}) = a - b\sqrt{3}$.
**Additive homomorphism.**

$$\varphi\big((a + b\sqrt{3}) + (c + d\sqrt{3})\big) = \varphi\big((a + c) + (b + d)\sqrt{3}\big) = (a + c) - (b + d)\sqrt{3} = \varphi(a + b\sqrt{3}) + \varphi(c + d\sqrt{3}).$$

**Multiplicative homomorphism.**

$$\begin{aligned}\varphi\big((a + b\sqrt{3})(c + d\sqrt{3})\big) &= \varphi\big((ac + 3bd) + (ad + bc)\sqrt{3}\big)\\ &= (ac + 3bd) - (ad + bc)\sqrt{3}\\ &= (a - b\sqrt{3})(c - d\sqrt{3})\\ = \varphi(a + b\sqrt{3})\,\varphi(c + d\sqrt{3}).\end{aligned}$$

**Bijective.** $\varphi$ is its own inverse: $\varphi(\varphi(z)) = z$ for all $z$. Hence $\varphi$ is bijective. 😄

### 4.1.3 (iii) Minimality of $\mathbb{Q}^{\sqrt{3}}$

**Example 4.1.3** (The field $\mathbb{Q}^{\sqrt{3}}$ is the smallest field containing $\mathbb{Q}$ and $\sqrt{3}$)

***Proof:*** Let $K$ be any field with $\mathbb{Q} \subseteq K$ and $\sqrt{3} \in K$. For $a, b \in \mathbb{Q} \subseteq K$ we have

$$a + b\sqrt{3} \in K$$

because $K$ is closed under the field operations. Thus $\mathbb{Q}^{\sqrt{3}} \subseteq K$. Since $K$ was arbitrary, $\mathbb{Q}^{\sqrt{3}}$ is contained in every such field, i.e. it is the smallest field containing $\mathbb{Q}$ and $\sqrt{3}$. 😄

### 4.1.4 (iv) Interpretation in terms of splitting fields

**Example 4.1.4** (The role of $\mathbb{Q}^{\sqrt{3}}$ in the theory of splitting fields)

***Proof:*** The polynomial $x^2 - 3$ has roots $\pm\sqrt{3}$. The field $\mathbb{Q}^{\sqrt{3}}$ contains both of them, hence it is a *splitting field* of $x^2 - 3$ over $\mathbb{Q}$. In general, for a polynomial $f \in \mathbb{Q}^x$ the smallest field containing all of its roots is called the splitting field of $f$. By analogy, the complex numbers $\mathbb{C}$ are the smallest field extension of $\mathbb{R}$ that contains the roots of *every* real polynomial; equivalently, $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. (Over $\mathbb{Q}$

the analogous minimal algebraically closed field is the field of algebraic numbers, a subfield of $\mathbb{C}$.) 😄

**Question 2: Problem 2. Characteristic $p$**

Let $\mathbb{F}$ be a field of characteristic $p$, meaning:

$$\underbrace{1 + \cdots + 1}_{p}$$

Prove that $(a+b)^p = a^p + b^p$ for all $a, b \in \mathbb{F}$