

Linear Algebra

Definition 1.1 (Group).

A *group* G is a set together with a map $*$: $G \times G \rightarrow G$ such that

- (i) $*$ is associative: $(a * b) \cdot c = s * (b * c) \quad \forall a, b, c \in G$,
- (ii) there exists an *identity element* $e \in G$ such that $a * e = e * a = a \quad \forall a \in G$,
- (iii) for every $a \in G$ there exists an *inverse element* $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = 1$.

If G is a finite set, we say that $(G, *)$ is a *finite group*. If $a * b = b * a$ for all $a, b \in G$, we say that $(G, *)$ is an *abelian group*. Whenever a subset $H \subset G$ forms a group with respect to $*$ it is called a *subgroup* of G .

Example 1.2. 1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all abelian groups with respect to the usual addition, where $e = 1$ and $a^{-1} = -a$.

- 2. $\mathbb{Z}_n \doteq \{0, 1, \dots, n-1\}$ is a finite abelian group with respect to addition modulo n for every $n \in \mathbb{Z}$. The identity element is 0 and the inverse of a is $n - a$.
- 3. Then the collection of all permutations of the elements of finite set forms a group under composition. Such groups are called *Symmetric groups* and if the set has n elements, the group is denoted by S_n .
- 4. The set $GL(n, \mathbb{R})$ of all real, invertible $n \times n$ matrices forms a group under matrix multiplication and the set of orthogonal matrices $O(n, \mathbb{R})$ is an example of a subgroup.

Proposition 1.3. *Let $(G, *)$ be a group. Then*

- 1. *the identity element is unique.*
- 2. *the inverse of any element is unique.*

3. $(a^{-1})^{-1} = a$ for all $a \in G$.
4. $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$.

Definition 1.4. A map $f : (G, *_G) \rightarrow (H, *_H)$ is called a *group homomorphism* if

$$f(a *_G b) = f(a) *_H f(b) \quad \forall a, b \in G.$$

Moreover, if f is bijective, we call it a *group isomorphism*. We say that two groups are *isomorphic* (denoted by \cong) whenever there exists a group isomorphism between them.

Definition 1.5 (Conjugacy classes, cosets and normal subgroup).
Let $(G, *)$ be a group.

1. The *conjugacy class* of $a \in G$ is defined to be

$$G_a \doteq \{g * a * g^{-1} \mid g \in G\}.$$

2. Given a subgroup $H \subset G$ and an element $g \in G$, we define the *left/right cosets* by

$$gH \doteq \{gh \mid h \in H\} \quad \text{and} \quad Hg \doteq \{hg \mid h \in H\}.$$

3. A subgroup $H \subset G$ is said to be *normal* if

$$gH = Hg \quad \forall g \in G.$$

Definition 1.6 (Quotient group).

Let N be a normal subgroup of $(G, *)$. Then the space of cosets

$$G/H \doteq \{gH \mid g \in G\}$$

forms a group under the operation

$$(g_1H) \cdot (g_2H) = (g_1 * g_2)H.$$

Example 1.7. 1. $2\mathbb{Z} \doteq \{0, 2, 4, \dots\}$ is a normal subgroup of \mathbb{Z} and $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$.

2. $\mathbb{R}/\mathbb{Z} \cong U(1) \doteq \{z \in \mathbb{C} : |z| = 1\}$.

Definition 1.8 (Group action).

Let $(G, *)$ be a group and X be a set. A *group action* of G on X is a map

$$G \times X \rightarrow X, \quad (g, x) \mapsto g \triangleright x$$

such that

- (i) $e \triangleright x = x \quad \forall x \in X$
- (ii) $(a * b) \triangleright x = a \triangleright (b \triangleright x) \quad a, b \in G.$

A group action is said to be *free* if

$$g \triangleright x = x \implies g = e.$$

A group action is said to be *transitive* if

$$\forall x, y \in X \exists g \in G : x = g \triangleright y.$$

Example 1.9. 1. Any group acts *freely* and *transitively* on itself by left (or right) multiplication.

- 2. Symmetric groups act on the set of vertices of polyhedra.
- 3. \mathbb{Z} acts on \mathbb{R} by translation by an integer, i.e.

$$n \triangleright x = x + n.$$

Such action is free but not transitive.

- 4. $GL(n, \mathbb{R})$ and its subgroups act on the vector space \mathbb{R}^n (by matrix multiplication).

Theorem 1.10 (Cayley's theorem).

Every group is isomorphic to a subgroup of a symmetric group.

Definition 1.11 (Ring).

A *ring* R is a set together with an *addition* $+: R \times R \rightarrow R$ and a multiplication $\times: R \times R \rightarrow R$ such that

- (i) $(R, +)$ is an abelian group,
- (ii) \times is associative,
- (iii) distributivity holds:

$$\begin{aligned} a \times (b + c) &= a \times b + a \times c & \forall a, b, c \in R \\ (a + b) \times c &= a \times c + b \times c & \forall a, b, c \in R. \end{aligned}$$

We say $(R, +, \times)$ is a *commutative ring* whenever the multiplication is also commutative. If there is an element $1 \in R$ such that $a \times 1 = 1 \times a = a$ for all $a \in R$, we say that $(R, +, \times)$ is a *unital ring*.

Example 1.12. 1. $(\mathbb{Z}, +, \cdot)$ is a unital commutative ring.

2. The set $\mathbb{R}[x]$ of polynomials with coefficients in any commutative ring R is itself a ring.

Definition 1.13 (Field).

A field is a unital commutative ring with $0 \neq 1$ such that all nonzero elements have a multiplicative inverse.

Example 1.14. 1. \mathbb{Q} , \mathbb{R} and \mathbb{C} are fields under the usual operations.

2. \mathbb{Z}_p is a finite (*Galois*) field if and only if p is prime.

Definition 1.15 (Vector space).

A *vector space* (or *linear space*) over a field \mathbb{K} (\mathbb{R} or \mathbb{C}) is a set V along with an *addition*

$$+ : V \times V \rightarrow V$$

and a *scalar multiplication*

$$\cdot : \mathbb{K} \times V \rightarrow V$$

satisfying

- (i) additive associativity: $(u + v) + w = u + (v + w) \quad \forall u, v, w \in V$
- (ii) additive identity: $\exists 0 \in V : v + 0 = v \quad \forall v \in V$
- (iii) additive inverse: $\forall v \in V \exists (-v) \in V : v + (-v) = 0$
- (iv) additive commutativity: $u + v = v + u \quad \forall u, v \in V$.
- (v) distributivity from the left: $\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v \quad \forall u, v \in V \text{ and } \lambda \in \mathbb{K}$
- (vi) distributivity from the right: $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v \quad \forall v \in V \text{ and } \forall \lambda, \mu \in \mathbb{K}$
- (vii) multiplicative associativity: $(\lambda \mu) \cdot v = \lambda \cdot (\mu \cdot v) \quad \forall v \in V \text{ and } \forall \lambda, \mu \in \mathbb{K}$
- (viii) multiplicative identity: $1 \in \mathbb{K} : 1 \cdot v = v \quad \forall v \in V$

If a set $W \subset V$ forms a vector space under the same operation, it is called a *linear subspace*.

Remark 1.16. Properties (i)-(iv) can be summarised as saying that V with its addition forms an Abelian group. Property (v) says that the map

$$\lambda \cdot : V \rightarrow V, v \mapsto \lambda \cdot v$$

is a group homomorphism for each $\lambda \in \mathbb{K}$. The remaining properties are equivalent to saying that the map

$$\mathbb{K} \rightarrow \text{Hom}_{\text{Grp}}(V, V), \lambda \mapsto \lambda \cdot$$

is a homomorphism of rings.

Definition 1.17 (Linear maps).

A map $f : V \rightarrow W$ between vector spaces (over the same field) is said to be *linear* if for all $\lambda \in \mathbb{K}$ and $u, v \in V$ it holds that

$$\begin{aligned} f(u + v) &= f(u) + f(v) \\ f(\lambda u) &= \lambda f(u). \end{aligned}$$

A bijective linear map is called a *linear isomorphism*. We define the *kernel* and the *image* of the linear map by

$$\ker L = \{v \in V : L(v) = 0\}$$

and

$$\operatorname{Im} f = \{w \in W : \exists v \in V, w = L(v)\}$$

respectively. The set of all linear maps between V and W is denoted by $\mathcal{L}(V, W)$.

Definition 1.18.

Let V be a vector space and $B = (v_1, v_2, \dots)$ a tuple of vectors in V . The tuple B is said to be *linearly independent* if for every tuple of scalars $(\lambda_1, \lambda_2, \dots, \lambda_n)$

$$\sum_{j=1}^n \lambda_j v_j = 0$$

implies $\lambda_j = 0, \forall j \in \{1, \dots, n\}$.

We say B *spans* V if any vector $v \in V$ can be written as a *linear combination* of elements of B , i.e. there exist scalars $\lambda_1, \dots, \lambda_n \in \mathbb{K}$, such that

$$v = \sum_{j=1}^n \lambda_j v_j.$$

We call B a *basis* of V if it is both linearly independent and spans V .

Theorem 1.19 (Dimension theorem). *Every vector space has a basis and all bases of a vector space have the same cardinality. This cardinality is called the dimension of the vector space.*

Two vector spaces are isomorphic if and only if they have the same dimension.

Proposition 1.20. *Every finite dimensional vector space over \mathbb{K} is isomorphic to \mathbb{K}^n for some $n \in \mathbb{N}$. Each choice of basis provides an isomorphism. A linear map $f : V \rightarrow W$ from an n -dimensional to an m -dimensional vector space can be represented by an $m \times n$ matrix.*

Remark 1.21. The definition of a basis presented here is also called Hamel-basis. In the context of infinite-dimensional vector spaces equipped with a topology one usually uses so called Schauder-bases instead.

- Example 1.22.** 1. \mathbb{R}^3 is a three dimensional vector space and the Cartesian coordinate vectors $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ and $e_3 = (0, 0, 1)$ form a basis.
2. \mathbb{C} is a one dimensional vector space over \mathbb{C} and a two dimensional vector space over \mathbb{R} .
3. The space $\mathbb{M}_{n,m}(\mathbb{K})$ of all $n \times m$ matrices is a vector space over \mathbb{K} with component-wise operations.
4. For any two vector spaces V and W it holds that $\mathcal{L}(V, W)$ is a vector space under point-wise operations.
5. The Polynomial ring $\mathbb{K}[X]$ is an infinite dimensional vector space and $(1, X, X^2, X^3, \dots)$ is a basis.
6. The space $C(\mathbb{R}, \mathbb{R})$ of continuous real-valued functions on \mathbb{R} is an infinite dimensional vector space with no countable basis.

Definition 1.23.

Let V be a vector space and W a subspace of V . The *quotient space* V/W is defined as the set of equivalence classes under the relation

$$u \sim v \iff u - v \in W$$

together with the natural addition and scalar multiplication.

Theorem 1.24 (Isomorphism Theorem).

Let $f: V \rightarrow W$ be a linear map. The quotient space $V/\ker(f)$ is isomorphic to $\text{Im}(f)$

Proposition 1.25.

Let V be a finite dimensional vector space and W a subspace of V . It holds that

$$\dim(V/W) = \dim(V) - \dim(W).$$

Theorem 1.26 (The Rank nullity theorem).

Let $f: V \rightarrow W$ be a linear map and suppose that V is finite dimensional. Then,

$$\dim(V) = \dim(\ker f) + \dim(\text{Im } f).$$

Definition 1.27 (Eigenvalues and eigenvectors).

Let $f \in \mathcal{L}(V, V)$ be a linear map. We say that a scalar λ is an *eigenvalue* of f with *eigenvector* $v \in V$ whenever

$$f(v) = \lambda v$$

holds. The linear subspace $\ker(f - \lambda \text{id}_V)$ is called the *eigenspace* of λ . The set of all eigenvalues $\sigma(f)$ is called the *spectrum* of f .

Definition 1.28 (Inner product).

An *inner product* on a vector space V over \mathbb{K} is a map $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{K}$ satisfying

1. $\langle v, w \rangle = \overline{\langle w, v \rangle}, \quad \forall v, w \in V.$
2. $\langle \lambda v + w, u \rangle = \lambda \langle v, u \rangle + \langle w, u \rangle, \quad \forall v, w, u \in V.$
3. $\langle v, v \rangle > 0, \quad \forall v \in V \setminus \{0\}.$

A vector space together with an inner product is called an *inner product space*.

Definition 1.29. Let $(V, \langle \cdot, \cdot \rangle)$ be an inner product space and $f \in \mathcal{L}(V, V)$. We denote by f^* the unique linear map that satisfies

$$\langle f(v), w \rangle = \langle v, f^*(w) \rangle, \quad \forall v, w \in V$$

it is called the adjoint of f . We call f *normal* if $f \circ f^* = f^* \circ f$ and *self-adjoint* if $f = f^*$.

Remark 1.30. In the finite dimensional case, all the above concepts have their matrix counterpart: once we fix a basis on each vector space, vectors and linear maps are uniquely represented by their component matrices.

Theorem 1.31 (Finite dimensional Spectral theorem). *Let V be a finite dimensional inner product space and consider a linear map $f \in \mathcal{L}(V, V)$. If f is normal, then there exists a basis of V consisting of eigenvectors of f .*