Chapter 1

Elements of Algebra

Definition 1.1 (Group)**.**
A *group* G is a set together with a map $*: G \times G \to G$ 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. $\mathbb{Z}_n \doteq \{0, 1, \ldots, n-1\}$ 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 $\mathrm{GL}(n, \mathbb{R})$ 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* $a, b \in G$.

Exercise 1.1. Proof Proposition 1.3.

Definition 1.4. A map $f : (G, *_G) \to (H, *_H)$ 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

$$(g_1 H) \cdot (g_2 H) = (g_1 * g_2)H\,.$$

Example 1.7. 1. $2\mathbb{Z} \doteq \{0, 2, 4, \ldots\}$ 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

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

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

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

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 not transitive nor free.

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* $+ : R \times R \to R$ and a multiplication $\times : R \times R \to R$ such that

(i) $(R, +)$ is an abelian group,

(ii) $\times$ is associative,

(iii) distributivity holds:

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

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*

$$+ : V \times V \to V$$

and a *scalar multiplication*

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

satisfying

(i) additive commutativity: $u + v = v + u \qquad \forall\, u, v \in V.$

(ii) additive and multiplicative associativity:

$$\begin{aligned} (u+v)+w &= u+(v+w) && \forall\, u, v, w \in V \\ (\lambda\mu)\cdot v &= \lambda \cdot (\mu \cdot v) && \forall\, v \in V \text{ and } \forall\, \lambda, \mu \in \mathbb{K} \end{aligned}$$

(iii) additive identity: $\exists\, 0 \in V \;:\; v + 0 = v \quad \forall v \in V$

(iv) multiplicative identity: $\exists\, 1 \in V \;:\; 1 \cdot v = v \quad \forall v \in V$

(v) additive inverse: $\forall\, v \in V\; \exists(-v) \in V \;:\; v + (-v) = 0$

(vi) distributivity:

$$\begin{aligned} \lambda \cdot (u+v) &= \lambda \cdot u + \lambda \cdot v && \forall\, u, v \in V \text{ and } \lambda \in \mathbb{K} \\ (\lambda+\mu)\cdot v &= \lambda \cdot v + \mu \cdot v && \forall\, v \in V \text{ and } \forall\, \lambda, \mu \in \mathbb{K} \end{aligned}$$

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

Remark 1.16. the six properties above are equivalent to the fact that V is an *abelian group* under the addition and that scalar multiplication $\lambda \cdot : V \to V$ is a *ring homomorphism* for any $\lambda \in \mathbb{K}$.

Definition 1.17.
A set of vectors $\beta = \{v_1, v_2, \ldots\}$ on a vector space V is said to be *linearly independent* if there exists a set of scalars $\{\lambda_1, \lambda_2, \ldots\}$, not all zero, such that

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots = 0\,.$$

Moreover, if any vector $v \in V$ can be written as a *linear combination* of elements of β, i.e.

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \ldots \quad \text{for some scalars } \lambda_1, \ldots, \lambda_n\,,$$

we call β a *basis* of V. The number of elements of β is called the *dimension* of V.

Example 1.18.
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 componentwise operations.
4. The space $L^2([0,1])$ of square integrable real functions on the unit interval is an infinite dimensional vector space and
$$\{e^{2\pi n x} \;:\; n \in \mathbb{N}\}$$
forms a basis (Fourier expansion).

Definition 1.19 (Linear maps)**.**
A map $L : V \to W$ between vector spaces (over the same field) is said to be *linear* whenever

$$L(\lambda \cdot v_1 + v_2) = \lambda \cdot L(v_1) + L(v_2)\,.$$

A bijective linear map is called a *linear isomorphism*. The space of all linear maps between V and W is denoted by $\mathcal{L}(V, W)$ and it has a vector space structure under pointwise operations. We define the *kernel* and the *image* of the linear map by

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

and

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

respectively.

Theorem 1.20 (The Rank nullity theorem)**.** *Let $L : V \to W$ be a linear map and suppose that V is finite dimensional. Then,*

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

Theorem 1.21. *Every finite dimensional vector space over is isomorphic to $\mathbb{R}^n$ for some $n \in \mathbb{N}$.*

Definition 1.22 (Eigenvalues and eigenvectors)**.**
Let $L \in \mathcal{L}(V, V)$ be a linear map. We say that a scalar λ is an *eigenvalue* of L with *eigenvector* $v \in V$ whenever

$$L(v) = \lambda v$$

holds. The linear subspace $\ker(L - \lambda \mathrm{id}_V)$ is called the *eigenspace* of λ.

Definition 1.23 (Inner product)**.**
An *inner product* on a vector space V over $\mathbb{K}$ is a map $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{K}$ 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 1.24.
Let $(V, \langle \cdot, \cdot \rangle$ be an inner product space. A linear map $L \in \mathcal{L}(V, V)$ is called *Hermitian* (*Symmetric*) if

$$\langle L(v), w \rangle = \langle v, L(w) \rangle, \qquad \forall v, w \in V,$$

it is called *positive definite* if

$$\langle L(v), v \rangle > 0, \qquad \forall v \in V.$$

Theorem 1.25 (Finite dimensional Spectral theorem)**.** *Let V be a finite dimensional complex (real) inner product space and consider a linear map $L \in \mathcal{L}(V, V)$. If L is Hermitian (symmetric), then there exists a basis of V consisting of eigenvectors of L.*

Remark 1.26. 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.

Exercises

1. (Proposition 1.3) Let $(G, *)$ be a group. Show the following statements:

(a) the identity element and the inverse of any element are unique.

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

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

2. (Cayley's Theorem) Prove that any group is a subgroup of a symmetric group.

3. Find an example of

(i) A nonabelian group with no more elements than 6.

(ii) A group action that is free but not transitive.

4. Let $L \in \mathcal{L}(V, W)$ be a linear map between vector spaces. Show the following:

(a) $\ker L$ and $\operatorname{Im} L$ are linear subspaces of V and W respectively.

(b) L is injective if and only if $\ker L = \{0\}$.

(c) If $\dim(V) = \dim(W)$, then L is injective if and only if it is surjective.

5. Let V, W be finite dimensional real vector spaces. Prove the following isomorphisms:

(i) $\mathbb{C} \cong \mathbb{R}^2$ ($\mathbb{C}$ as a real vector space).

(ii) $\mathcal{L}(\mathbb{R}, \mathbb{R}^n) \cong \mathbb{R}^n$.

(iii) V $\cong \mathbb{R}^n$ for some $n \in \mathbb{N}$.

(iv) $\mathcal{L}(V, W) \cong \mathbb{R}^{dim(V) \times \dim(W)}$.

6. Consider three maps $f, g, h : \mathbb{R}^2 \to \mathbb{R}^2$ acting as shown in the image below. Select whether the following statements are true or false.

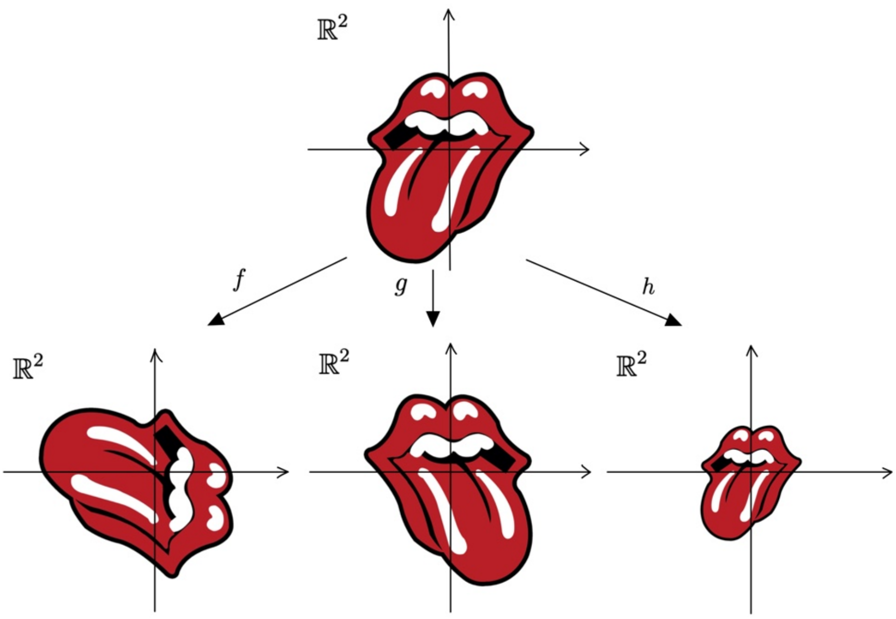
(i) f and h are linear but g is not.

(ii) f and g are linear but h is not.

(iii) f has a positive real eigenvalue.

(iv) g has a unique real eigenvalue.

(v) Any vector of $\mathbb{R}^2$ is an eigenvector of h.


$\mathbb{R}^2$
f
g
h
$\mathbb{R}^2$
$\mathbb{R}^2$
$\mathbb{R}^2$