

Glossary: Higher Linear Algebra: Definitions and Theorems

Dylan Wang (z5422214)

May 2023, Term 2

Definition. Groups.

A group G is a non-empty set with a binary operation defined on it. That is

1. Closure: for all $a, b \in G$ a composition $a * b$ is defined and in G .
2. Associativity: for all $a, b \in G$, $(a * b) * c = a * (b * c)$.
3. Identity: There is an element $e \in G$ such that $a * e e * a = a$.
4. Inverse: for each $a \in G$ there exists an $a' \in G$ such that $a * a' = a' * a = e$.

If G is a finite set then the order of G is $|G|$, the number of elements in G . Technically, a group is the pair $(G, *)$; said as “the group G under the operation $*$ ”.

*It captures the idea of a collection of objects, and came from symmetry; think about actions on a structure, and composing these actions.

Definition. Abelian Group.

A group G is abelian if the operation satisfies the commutative law

$$a * b = b * a \quad \text{for all} \quad a, b \in G.$$

Notes on Groups

- A composition is a function $* : G \times G \rightarrow G$.
- The operation $*$ is not restricted to but it is commonly addition (for abelian groups), multiplication (often written as juxtaposition) or composition of functions.
- We use power notation for repeated compositions: $a * a * a * \dots * a = a^n$ and $a^{-n} = (a^{-1})^n$.

Examples

- $(\mathbb{Z}, +)$ is an abelian group;
- $(\mathbb{Z}, -)$ is not a group because the inverse of 2 (or any $n \in \mathbb{Z}, n \neq \pm 1$) is not an integer.
- For any integer m , the set $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$ of remainders modul m is a group under addition modulo m .
- If p is prime, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication modulo p . This only works for primes because non-primes will lead to a zero result (e.g. $p = 6, 2 * 3 = 6 \bmod 6 = 0$.)
- For any set S , the set F of bijective functions $f : S \rightarrow S$ is a group under composition, but is not in general abelian.

Lemma. Properties of a Group.

Let $(G, *)$ be a group.

- There is only one identity element in G .
- Each element of G has only one inverse.
- For each $a \in G$, $(a^{-1})^{-1} = a$.
- For every $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$.
- Let $a, b, c \in G$. Then if $a * b = a * c$, $b = c$. Similarly, if $b * a = c * a$ then $b = c$.

Example. Let m be a positive integer and consider the set

$$C_m = \{e, a, a^2, a^3, \dots, a^{m-1}\},$$

where a is some (undefined) symbol.

Define an operation on C_m by specifying that $a^0 = e$ (soon; $a^m = e$) and

$$a^k * a^l = \begin{cases} a^{k+l} & \text{if } k+l < m \\ a^{k+l-m} & \text{otherwise} \end{cases}.$$

This is an abelian group known as a cyclic group of order m and we often write C_m as $\langle a : a^m = e \rangle$ and say it is generated by a .

Definition. Permutation Groups.

Let $\Omega_n = \{1, 2, \dots, n\}$. As an ordered set, Ω_n has $n!$ arrangements or permutations. If we think of these as functions, then each permutation is a bijection on Ω_n (mapping indices).

Then the set \mathcal{S}_n of all permutations of n objects forms a group under composition of order $n!$. The proof follows from the bijective function on a set example.

Definition. Small Finite Groups.

A Cayley table shows the compositions associated with a group, usually for small, finite groups.

Each row must be a permutation of the elements of the group, because:

- If we had a repetition in a row (or column), so that $x * a = x * b$, then the cancellation rule will give $a = b$.
- If $a^2 = a$ then composing with a^{-1} gives $a = e$, so the identity is the only element that can be fixed.

Example.

Example 1.5 *Let G be the set of matrices*

$$\left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Show that G is an abelian group under matrix multiplication and write out its multiplication table.

SOLUTION: Multiplying we get:

	I	A	B	C
I	I	A	B	C
A	A	\underline{I}	C	B
B	B	C	\underline{I}	A
C	C	B	A	$\underline{\underline{I}}$

2020 — p. 14

Definition. Fields.

A field $(\mathbb{F}, +, \times)$ is a set \mathbb{F} with two binary operations on it, addition $(+)$ and multiplication (\times) , where

1. $(\mathbb{F}, +)$ is an abelian group;
2. $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is an abelian group under multiplication, with 1 being the multiplicative identity;
3. The distributive laws $a \times (b + c) = a \times b + a \times c$ and $(a + b) \times c = a \times c + b \times c$ hold.

Note this satisfies the $12 = 5 + 5 + 2$ number laws.

*It is called a ‘field’ to resemble fields in physics; that is, a premise upon which there is rich structure and interplay.

Lemma. Interplay Between $+$ and \times .

Let \mathbb{F} be a field and $a, b, c \in \mathbb{F}$. Then

- $a0 = 0$ (additive identity);
- $a(-b) = -(ab)$ (associativity);
- $a(b-c) = ab - ac$ (distributive law);
- if $ab = 0$ then either $a = 0$ or $b = 0$ (proof: suppose $ab = 0$ and $a \neq 0$, then multiply both sides by a^{-1} to give $0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$).

Definition. Subgroups.

Let $(G, *)$ be a group and H a non-empty subset of G .

Then H is a subgroup of G if H is a group under the restriction of $*$ to H .

We write this as $H \leq G$ and say H inherits the group structure from G .

*The idea is that H is just a smaller bunch of objects within G , the whole collection, and also has its structure and properties.

Lemma. The Subgroup Lemma.

Let $(G, *)$ be a group and H a non-empty subset of G .

Then H is a subgroup of G if and only if

- for all $a, b \in H$, $a * b \in H$;
- for all $a \in H$, $a^{-1} \in H$;

These are all proved from closure and inverse of the group; associativity is inherited from G and an identity exists via the inverse.

Note that any subgroup of an abelian group is also an abelian group.

Examples

1. Every non-trivial group G has at least two subgroups: $\{e\}$ and G .
2. For any integer m let $m\mathbb{Z}$ be the set of all multiples of m . Then $(m\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.
The converse is also true; any subgroup of $(\mathbb{Z}, +)$ is $(m\mathbb{Z}, +)$ for some m .
3. Consider $C_m = \langle a : a^m = e \rangle$ the cyclic group of order m .
Picking any integer k with $1 < k < m$ we could generate a subgroup $H_k = \langle a^k \rangle$ of C_m by looking at all powers of a_k . Clearly, the order of H_k cannot be larger than m ; it is strictly less than m if and only if k and m have a common divisor $d > 1$.
4. Let $n \geq 1$ be any integer. The set of invertible $n \times n$ matrices over a field \mathbb{F} is a group under matrix multiplication. It is non-abelian if $n > 1$. It is called the general linear group $\text{GL}(n, \mathbb{F})$.
They have important subgroups, such as the special linear groups $\text{SL}(n, \mathbb{R})$ and $\text{SL}(n, \mathbb{C})$ of matrices with determinant 1, and the group of orthogonal matrices $O(n) \leq \text{GL}(n, \mathbb{R})$.

Definition. Subfields.

If $(\mathbb{F}, +, \times)$ is a field and $\mathbb{E} \subseteq \mathbb{F}$ is also a field under the same operations, then $(\mathbb{E}, +, \times)$ is a subfield of $(\mathbb{F}, +, \times)$, usually written $\mathbb{E} \leq \mathbb{F}$.

Lemma. The Subfield Lemma.

Let $\mathbb{E} \neq \{0\}$ be a non-empty subset of field \mathbb{F} .

Then \mathbb{E} is a subfield of \mathbb{F} if and only if for all $a, b \in \mathbb{E}$

$$a + b \in \mathbb{E}, \quad -b \in \mathbb{E}, \quad a \times b \in \mathbb{E}, \quad b^{-1} \in \mathbb{E} \text{ if } b \neq 0.$$

Proof: The distributive laws are inherited from \mathbb{F} , and the rest of the proof comes from applying the subgroup lemma to $(\mathbb{E}, +)$ and (\mathbb{E}, \times) .

Definition. Morphisms.

Let $(G, *)$ and (H, \circ) be two groups. A (group) homomorphism from G to H is a map $\phi : G \rightarrow H$ that respects the two operations, that is where

$$\phi(a * b) = \phi(a) \circ \phi(b) \quad \text{for all } a, b \in G.$$

A bijective homomorphism $\phi : G \rightarrow H$ is called an isomorphism; the groups are then said to be isomorphic, and are considered the same group. isomorphism is an equivalence relation.

*The word ‘homomorphism’ comes from the Ancient Greek language: homos meaning “same” and morphe meaning “form” or “shape”.

**Homomorphic maps preserve the structure of the domain group while respecting that of the codomain. The idea is if $a * b$, then under the map ϕ , we hope that (mapped) a behaves the same with (mapped) b in the codomain. If so, they are homomorphic.

Example. Let $m \geq 2$ be any integer. Define $\phi : (\mathbb{Z}, +) \rightarrow (m\mathbb{Z}, +)$ by $\phi(a) = ma$. Show that ϕ is an isomorphism of groups.

Solution. Firstly

$$\phi(a + b) = m(a + b) = ma + mb = \phi(a) + \phi(b).$$

The easiest way to show ϕ is a bijection is to find the inverse. But if $g \in m\mathbb{Z}$ then $g = ma$ for some $a \in \mathbb{Z}$ and clearly $\phi(a) = g$, so $\phi^{-1}(g) = a$. Thus ϕ is an isomorphism.

Lemma. Homomorphism Lemma.

Let $(G, *)$ and (H, \circ) be two groups and ϕ a homomorphism between them. Then

- ϕ maps the identity of G to the identity of H .
- ϕ maps inverses to inverses, i.e. $\phi(a^{-1}) = (\phi(a))^{-1}$ for all $a \in G$.
- if ϕ is an isomorphism from G to H then ϕ^{-1} is an isomorphism from H to G .

Definition. Kernel and Image.

Let $\phi : G \rightarrow H$ be a group homomorphism, with e' the identity of H .

The kernel of ϕ is the set

$$\ker(\phi) = \{g \in G : \phi(g) = e'\}.$$

It is the information lost in the map.

The image of ϕ is the set

$$\text{im}(\phi) = \{h \in H : h = \phi(g), \text{ for some } g \in G\}$$

.It is the approximation given by the map.

Lemma. Kernel and Image Lemma.

For $\phi : G \rightarrow H$ a group homomorphism, $\ker(\phi) \leq G$ and $\text{im}(\phi) \leq H$.

Lemma. Isomorphism Lemma.

A homomorphism ϕ is one-to-one if and only if $\ker(\phi) = \{e\}$, with e the identity of G . If ϕ is one-to-one then $\text{textim}(\phi)$ is isomorphic to G .

Definition. Linear Representation of G on \mathbb{F}^n .

If there exists a homomorphism $\phi : G \rightarrow \text{GL}(n, \mathbb{F})$ for some n and some field \mathbb{F} , then the group $\text{im}(\phi)$ is called a linear representation of G on \mathbb{F}^n .

If ϕ is one-to-one (so every element maps to a distinct matrix), we call the representation faithful.

Definition. Permutation Representation.

From above, in the case where G is finite and H is S_n for some n , then we get a permutation representation of the group G as a subgroup of S_n .

Definition. Vector Space.

Let \mathbb{F} be a field. A vector space over the field \mathbb{F} consists of an abelian group $(V, +)$ and a function from $\mathbb{F} \times V$ to V called scalar multiplication and written $\alpha \mathbf{v}$ where

1. $\alpha(\beta \mathbf{v}) = (\alpha\beta) \mathbf{v}$ for all $\alpha, \beta \in \mathbb{F}$ and $\mathbf{v} \in V$.
2. $1 \mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$.
3. $\alpha(\mathbf{u} + \mathbf{v}) = \alpha \mathbf{u} + \alpha \mathbf{v}$ for all $\alpha \in \mathbb{F}$ and $\mathbf{u}, \mathbf{v} \in V$.
4. $(\alpha + \beta) \mathbf{u} = \alpha \mathbf{u} + \beta \mathbf{u}$ for all $\alpha, \beta \in \mathbb{F}$ and $\mathbf{u} \in V$.

There are ten axioms here; 5 from the abelian group, closure of scalar multiplication, and four explicit ones. The $+$ in $(V, +)$ may be distinguished as vector addition.

Lemma. 2.1.

Let V be a vector space over field \mathbb{F} . For all $\mathbf{v}, \mathbf{w} \in V$ and $\lambda \in \mathbb{F}$ then

- $0 \mathbf{v} = \mathbf{0}$ and $\lambda \mathbf{0} = \mathbf{0}$.
- $(-1) \mathbf{v} = -\mathbf{v}$.
- $\lambda \mathbf{v} = \mathbf{0}$ implies either $\lambda = 0$ or $\mathbf{v} = \mathbf{0}$.
- If $\lambda \mathbf{v} = \lambda \mathbf{w}$ and $\lambda \neq 0$ then $\mathbf{v} = \mathbf{w}$.

Standard Vector Space Examples.

1. n -tuples.

The set \mathbb{F}^n consists of all n -tuples of elements of \mathbb{F} :

$$\mathbb{F}^n = \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} : \alpha_i \in \mathbb{F} \right\}.$$

If $\mathbf{x} = (\alpha_i)_{1 \leq i \leq n}$, $\mathbf{y} = (\beta_i)_{1 \leq i \leq n}$ are elements of \mathbb{F}^n , then vector addition on \mathbb{F}^n is defined as $\mathbf{x} + \mathbf{y} = (\alpha_i + \beta_i)_{1 \leq i \leq n}$.

Scalar multiplication on \mathbb{F}^n is $\lambda \mathbf{x} = (\lambda \alpha_i)_{1 \leq i \leq n}$.

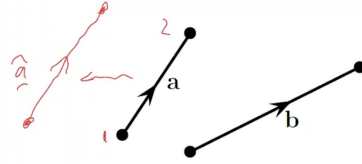
With these operations, \mathbb{F}^n is a vector space over \mathbb{F} .

You met \mathbb{R}^n in first year – mainly \mathbb{R}^2 and \mathbb{R}^3 of course – and you should be familiar with those vector spaces.

2. Geometric Vectors.

2. Geometric vectors

Geometric vectors are ordered pairs of points in \mathbb{R}^n , joined by labelled arrows.



We add these objects by placing them head to tail and scalar multiplying is just stretching the vector's length while preserving the direction (or reversing if the scalar is negative).

The set of all geometric vectors do not form a vector space. However, if you define 2 geometric vectors to be **equivalent** if one is a translation of the other then **the set of equivalence classes of geometric vectors** is a vector space.

3. Matrices.

For any positive integers p and q the set $M_{p,q}(\mathbb{F})$ is the set of $p \times q$ matrices with elements from \mathbb{F} . Then $M_{p,q}(\mathbb{F})$ is a vector space over \mathbb{F} with vector addition with the usual addition of matrices and scalar multiplication multiplying each element of the matrix.

4. Polynomials.

The set of all Polynomials with coefficients in \mathbb{F} , $\mathcal{P}(\mathbb{F})$, is a vector space over \mathbb{F} with

$$(f + g)(x) = f(x) + g(x) \quad \text{for all } x \text{ in } \mathbb{F} \quad (\lambda f)(x) = \lambda f(x) \quad \text{for all } \lambda, x \in \mathbb{F}.$$

Similarly, $\mathcal{P}(F)$ (polynomials of degree n or less) is a vector space over \mathbb{F} . Note this example shows 'vector spaces' can appear abstract from actual vectors! We just need vector $+$ and \times .

5. Function Spaces.

Let X be a non-empty set and \mathbb{F} be a field. Then define

$$\mathcal{F}[X] = \{f : X \rightarrow \mathbb{F}\}.$$

The set $\mathcal{F}[X]$ is a vector space over \mathbb{F} if we define

- the zero in $\mathcal{F}[X]$ to be the zero function: $x \rightarrow 0$ for all $x \in X$.
- $(f + g)(x) = f(x) + g(x)$ for all $x \text{ in } X$.
- $(\lambda f)(x) = \lambda(f(x))$ for all $x \in X$.