Higher Linear Algebra
MATH2601 UNSW

Jeremy Le
(Based of Hussain Nawaz's Notes)

2023T2

Contents

1 Group and Fields

1.1 Groups

Definition 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:** $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$,
3. **Identity:** there is an element $e \in G$ such that $a * e = e * a$ for all $a \in G$,
4. **Inverse:** for each $a \in G$ there is 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.

Groups are defined as $(G, *)$. We say this as "the group G under the operation $*$".

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

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

Notation

- We use power notation for repeated applications: $a * a \cdots * a = a^n$ and $a^{-n} = (a^{-1})^n$.
- For group operation, $\times$ we use 1 for the identity and a^{-1} for inverse of a.
- For group operation, $+$ we use 0 for the identity and $-a$ for the inverse of a.
- We would then write na for $a + a + \cdots a$ (repeated addition, not multiplying by n).

Trivial Groups The trivial group is the group consisting of exactly one element, $\{e\}$. It is the smallest possible group, since there has to be at least one element in a group.

More Properties of Groups

- There is only one identity element in G.
- Each element of G only has 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 $a * b = a * c, b = c$.

1.1.1 Permutation Groups

Let $\Omega_n = \{1, 2, \ldots, n\}$. As an ordered set $\Omega_n = (1, 2, \ldots, n)$ has $n!$ rearrangements. We may think of these permutations as being functions $f : \Omega_n \to \Omega_n$. These are bijections.

Observe that the set $\mathcal{S}_n$ of all permutations of n objects forms a group under composition of order $n!$.

Small Finite Groups Small groups can be pictured using a multiplication table, where the row element is multiplied on the left of the column element.

In a multiplication table of finite group each row must be a permutation of the elements of the group, because:

- If we had repetition in a row (or column), so that $xa = xb$, then the cancellation rule will give $a = b$. Hence each element occurs no more than once in a row (or column).
- If $a^2 = a$ then multiplying by a^{-1} gives $a = e$, so the identity is the only element that can be fixed.

1.2 Fields

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

1. $(\mathbb{F}, +)$ is an abelian group,
2. $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is an abelian group under multiplication,
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.

Additional Notes

- Our definition is equivalent to saying $\mathbb{F}$ satisfies the $12 = 5 + 5 + 2$ number laws.
- We use juxtaposition for the multiplication in fields and 1 for the identity under multiplication.
- The smallest possible field has two elements, and is written $\{0, 1\}$ with $1 + 1 = 0$.

Finite Fields The only finite fields are those of size p^k for some prime p (referred to as the characteristic of the field) and positive integer k. These fields are called Galois fields of size p^k, $\mathrm{GF}(p^k)$. Note that $\mathrm{GF}(p^k) \neq \mathbb{Z}_{p^k}$ unless $k = 1$.

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

- $a0 = 0$
- $a(-b) = -(ab)$
- $a(b - c) = ab - ac$
- if $ab = 0$ then either $a = 0$ or $b = 0$.

1.3 Subgroups and Subfields

Subgroups Let $(G, *)$ be a group and H a non-empty subset of G. If H is a group under the restriction of $*$ to H, we call it a subgroup of G. We write this as $H \leq G$ and say H inherits the group structure from G.

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

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

i.e. H is closed under $*$ and $^{-1}$.

Note that every non-trivial group G has at least two subgroups: $\{e\}$ and G.

General Linear Groups Let $n \geq 1$ be an integer. The set of invertible $n \times n$ matrices over field $\mathbb{F}$ is a group under matrix multiplication. This is a special case of a bijection function $f : S \to S$ with $S = \mathbb{F}^n$ and is non-abelian if $n > 1$.

It is called the general linear group, $\mathrm{GL}(n, f)$.

The groups $\mathrm{GL}(n, \mathbb{R})$ and $\mathrm{GL}(n, \mathbb{C})$ are especially important in this course. They have many important subgroups, such as

- the special linear groups $\mathrm{SL}(n, \mathbb{R})$ and $\mathrm{SL}(n, \mathbb{C})$ of matrices with determinant 1.
- $O(n) \leq \mathrm{GL}(n, \mathbb{R})$ the group of orthogonal matrices.
- $\mathrm{SO}(n) = O(n) \cap \mathrm{SL}(n, \mathbb{R})$ of special orthogonal matrices.

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

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 iff for all $a, b \in \mathbb{E}$:

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

Rational + Irrational Field Let α be any (non-rational) real or complex number. We defined $\mathbb{Q}(a)$ to be the smallest field containing both $\mathbb{Q}$ and α. Such fields are important in number theory and can clearly be generalised to e.g. $\mathbb{Q}(\alpha, \beta)$. For example, it can be shown

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

1.4 Morphisms

A morphism is a category of "nice" maps between the members.

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

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

Isomorphism A bijective homomorphism $\phi : G \to H$ is called an isomorphism: the groups are then said to be isomorphic. That is, $G \cong H$.

Isomorphism Lemmas 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 inverse, 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.

Images and Kernel Let $\phi : G \to H$ be a group homorphism, with e' the identity of H. The kernal of ϕ is the set

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

The image of ϕ is the set

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

Note that $\ker \phi \leq G$ and $\text{im}\, \phi \leq H$.

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

Linear Groups A common use of group homomorphisms is to look for a homomorphism $\phi : G \to \text{GL}(n, \mathbb{F})$ for some n and some field $\mathbb{F}$. The group $\text{im}(\phi)$ is called a (linear) representation of G on $\mathbb{F}^n$. If ϕ is one-one (so every element maps to a distinct matrix), we call the representation faithful.

2 Vector Spaces

2.1 Vector Spaces

Motivation for Vector Spaces The concept of a vector space is a natural and important generalisation of $\mathbb{R}^n$. It is natural to consider them whenever possible to add objects and multiply them by scalars.

It may be convenient to consider a field $\mathbb{F}$ as a vector space over one of its subfields.

Vector Spaces Let $\mathbb{F}$ be a field. A vector space over the field $\mathbb{F}$ consists of an abelian group $(V, +)$ plus 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 $\alpha, \beta \in \mathbb{F}$ for all $\mathbf{v} \in V$.
2. $1\mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$.
3. $\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{u}$ for all $\alpha \in \mathbb{F}$ for all $\mathbf{u}, \mathbf{v} \in V$.
4. $(\alpha + \beta)\mathbf{u} + \alpha\mathbf{u} + \beta\mathbf{u}$ for all $\alpha, \beta \in \mathbb{F}$ for all $\mathbf{u} \in V$.

Properties and Notation for Vector Spaces dsdfa

1. There are ten axioms here: 5 from the abelian group, closure of scalar multiplication and the four explicit ones.
2. Addition in V is called vector addition to distinguish it from the addition in $\mathbb{F}$.
3. Being a group, V cannot be empty.
4. Bold face letters are used to distinguish elements of V from elements of $\mathbb{F}$.

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

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

2.2 Standard Examples of Vector Spaces

The Space $\mathbb{F}^n$ over $\mathbb{F}$ 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 $\mathbb{F}$.

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.

The set of all geometric vectors does 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.

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

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

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

Similarly, $\mathcal{P}_n(F)$ (polynomials of degree n or less) is a vector space over $\mathbb{F}$.

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

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

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: $x \to 0$ for all $x \in X$
- $(f+g)(x) = f(x) + g(x)$ for all $x \in X$
- $(\lambda f)(x) = \lambda(f(x))$ for all $x \in X$