Higher Linear Algebra
Notes — Math2601 UNSW

Hussain Nawaz
hussain.nwz000@gmail.com

2022T2

Contents

1 Groups and Fields

1.1 Groups

Definition of Groups A group G is a non-empty set with a binary operation defined on it. It must satisfy the following four properties:

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).
3. **Identify:** There exists an $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.
4. **Inverse:** For all $a \in G$, there exists an a' such that $a * a' = a' * a = e$.

Groups Order and Pair Groups are actually pairs of objects. The first is the set of elements in the group and the second, the operation defined on the group. Therefore, groups may be written as $(G, *)$.

If G is finite, then the order of G, that is $|G|$, is the number of element in G.

Abelian Groups A group is abelian if the operation is *commutative*. That is,

$$a * b = b * a \quad \forall a, b \in G.$$

Notes on the Composition Observe that the composition is actually a function $* : G \times G \to G$. $a * b$ is simply a more convenient notation than $*(a, b)$.

Though the operation $*$ is not restricted, it is often one of addition (only for abelian groups), multiplication ($\times$, often written as juxtaposition) or, composition of functions.

Notation for Repeated Composition We may often use power notation for repeated applications of a composition. That is, $a * a * \cdots * a$ (with n compositions) may be written as a^n.

Suppose that instead we are using $+$ as the group operation, then $a + a + \cdots + a$ (added n times), may be written as na. Do note that this is <u>not</u> multiplication.

Trivial Groups The trivial group consists of exactly one element, the identity. That is, $\{e\}$. Since the empty set cannot be a group, as there is required to be at least one element in a group, the trivial group is the smallest group that exists.

Examples of Groups $(\mathbb{Z}, +)$ is an abelian group under the usual addition operation. However, $(\mathbb{Z}, \times)$ is not a group, since the inverse property cannot be satisfied. Similarly, $(, \times)$ is also not a group as 0 has no multiplicative inverse. However $(\mathbb{R} \backslash 0)$ is a group.

For an integers in the set $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ is a group under addition, modulo m.

Function Composition and Groups For any S, the set F of bijective functions $f : S \to S$ is a group under composition but, it is not necessarily abelian.

Proof Composing two bijections gives a bijection so, the operation is closed. Associativity is of composition follows as

$$(f \circ (g \circ h))(x) = f(g(h(x))) = (f \circ g) \circ h(x).$$

The identity function is $e(x) = x$ is a clear bijection. The inverse exists by definition of the bijection.

More Properties of Groups

- There is only *one* inverse of each element. That is, the inverse is unique.
- For all $a \in G$, $(a^{-1})^{-1} = a$
- For all $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$.
- let $a, b, c \in G$. Then if $a*b = a*c$, then $b = c$. We may think of this as the cancellation property.

Permutation Groups Let $\Omega_n = \{1, 2, \dots, n\}$. As a ordered set, Ω_n has $n!$ permutations.

We may think of these permutations as being functions $f : \Omega_n \to \Omega_n$. Clearly, these are bijections.

Observe that the set S_n of all permutations forms a group under the composition of order n as, the set of all bijections on a set is a group.

We may write these permutations f as a matrix where, the i, j entry represents how what element is mapped to the j-th index, by f_i.

Small Finite Groups We may visualise these with a multiplication table where, the row element is multiplied on the left of the column element.

In a multiplication table of a finite group, each row must be a permutation of the elements of the group. Otherwise, if there was a repetition in a row then $xa = xb$ implies $a = b$ by the cancellation property. Thus, each element occurs no more than once is a row.

If $a^2 = a$ then, by cancellation property, $a = e$. So, the identity must be the only element that is fixed.

1.2 Fields

Definition of Fields A field is a set $\mathbb{F}$ with two binary operations on it, addition $(+)$ and, multiplication, $(\times)$ such that, the following hold

1. $(\mathbb{F}, +)$ is an abelian group.
2. $(\mathbb{F}^* \backslash \{0\}, \times)$ is an abelian group, where 0 is the additive 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.

Fields and Notation

- Under the obvious operations, typically refer to the field as just $\mathbb{F}$.
- We use juxtaposition for multiplication under fields and, 1 as the multiplicative identify and often 0 as the additive identity.
- By our definition of fields as groups, it is equivalent to say that if $\mathbb{F}$ is a field then, it satisfies the $12 = 5 + 5. + 2$ number laws.
- The smallest possible fields only has two elements, the multiplicative and additive identity. That is, $\{0, 1\}$.
- We let $-b$ be the inverse of b under addition and may write $a + (-b)$ as $a - b$ as a shorthand. Similarly, we may write $\frac{a}{b}$ rather than ab^{-1} where b^{-1} is the multiplication inverse and $b \neq 0$.

Finite Fields The only finite fields that exists are those of the size p^k for some positive integer k and prime p (also known as, the characteristic of the field).

These may be called *Galois fields* of size p^k. That is, $GF(p^k)$. Note that $GF(p^k) \neq \mathbb{Z}_{p^k}$ unless $k = 1$.

Properties of Fields If $\mathbb{F}$ is 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

Defining Subgroups Let $(G, *)$ be a group and H be a non-empty subset of G. Suppose that $(H, *)$ satisfies the requirements of a group, then it is a subgroup of G.

We may write $H \leq G$ such that H inherits the group structure from G.

The Subgroup Lemma Let $(G, *)$ be a group and H a non-empty subset of G. H is a subgroup if and only if

1. $a * b \in H \quad \forall a, b \in H$
2. $a^{-1} \in H \quad \forall a \in H$

That is, H is closed under $*$ and ${}^{-1}$.

Associativity for the subset follows from associativity of the group structure. The identity also follows from the closure under an inverse and multiplication since $a^{-1} * a = e \in H$.

Note that every non-trivial group G will have two subgroups. They are the $\{e\}$ and G.

General Linear Groups Let n be an integer such that $n \geq 1$. The set of invertible $n \times n$ matrices over $\mathbb{F}$ is a group under the operation of matrix multiplication. This is a special case of a bijection function $f : S \to S$ with $S = \mathbb{F}^n$. This group will be non-abelian if $n > 1$. This group is names the *General Linear Group*, denoted as $GL(n, \mathbb{F})$

Special Linear Group The special linear groups are a subset of the general linear groups denoted as $SL(n, \mathbb{F})$ with the requirement that the matrices all have a determinant of $\mathbb{R}$.

Orthogonal Matrix Group The set of $n \times n$ orthogonal matrices over $\mathbb{F}$ is a subgroup of $GL(n, \mathbb{F})$.

That is, $O(n) \leq GL(n, \mathbb{R})$.

There also exists $SO(n) = O(n) \cap SL(n, \mathbb{R})$ which is the intersection of the orthogonal matrices and special matrices which is also a group.

Subfields Let $(\mathbb{F}, +, \times)$ be a field and $\mathbb{E} \subseteq \mathbb{F}$ such that $\mathbb{E}$ is also a field under the same operations.

Then, $(\mathbb{E}, +, \times)$ is a subfield of $\mathbb{F}$. Equivalently, $\mathbb{E} \leq \mathbb{F}$.

Subfield Lemma Let $\mathbb{E} \neq \{0\}$ be a non-empty subset of a field $\mathbb{F}$. Then, $\mathbb{E}$ is a subfield of $\mathbb{F}$ if and only if, for all $a, b \in \mathbb{E}$,

1. $a + b \in \mathbb{E}$,
2. $-b \in \mathbb{E}$,
3. $a \times b \in \mathbb{E}$,
4. $b^{-1} \in \mathbb{E}$ given $b \neq 0$.

The distributive laws are inherited from $\mathbb{F}$ and need no checking. The rest of the proof may follow from applications of the subgroup lemma to each operation $\mathbb{E}, +$ and $\mathbb{E}, \times$.

Cool Rational + Irrational Alpha Field Let α be any non-rational real or complex number. We may define $\mathbb{Q}(\alpha)$ to be the smallest field containing both $\mathbb{Q}$ and α.

The smallest such field is of the form $\{a + b\alpha : a, b \in \mathbb{Q}\}$.

1.4 Morphisms

Morphisms are the *nice* maps between the members.

Homomorphism Definition 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,

$$\phi(a * b) = \phi(a) \circ \phi(b) \quad \forall a, b \in G$$

Isomorphism An isomorphism is a bijective homomorphism $\phi : G \to H$. The groups are then isomorphic. That is, $G \cong H$.

In terms of group theory, if two groups are isomorphic then, they are effectively the same group. Isomorphism is an equivalence relation on groups.

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

Images and Kernel Definition Let $\phi : G \to H$ be a group homomorphism with, e' the identity of H.

The kernel of ϕ is the set

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

Observer that $\ker \phi \leq G$.

The image of ϕ is the set

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

Note that $\text{im}\phi \leq G$.

One-to-One Homomorphisms A homomorphism is one-to-one if and only if $\ker \theta = \{e\}$, where e is the identity of G.

If ϕ is one-to-one then, $\text{im}(\phi)$ is isomorphic to G.

Group Homomorphisms and General Linear Group It is common to seek a homomorphism $\phi : G \to GL(n, \mathbb{F})$ for some n and field $\mathbb{F}$.

If ϕ is one to one (each element maps to a unique matrix), then the representation is faithful.

Example of Group Homomorphisms on GL Consider $C_4 = \{e, a, a^2, a^3\}$ $(a^4 = e)$. Let $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Define $\phi : C_4 GL(2, \mathbb{R})$ by $\phi(a^k) = J^k$.

Then, ϕ is a faithful representation of C_4 on $\mathbb{R}^2$.

Often, we may represent to the image subgroup of matrices as the group itself.

Cayley's Theorem We may apply the lemma that $\text{im}(\phi)$ is a subgroup, to the case where G is finite and H is S_n for some n.

In this case, we get a permutation representation of the group G as a subgroup of S_n.

Cayley's theorem states that every finite group G has a representation as a subgroup of S_n for $n \leq |G|$. That is, S_n and its subgroups are all that exists in the case of finite groups.