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 $b = 0$.