Algebraic Structures

Properties

- **Associativity**
  (a · b) · c = a · (b · c)
- **Commutativity**
  a · b = b · a
- **Distributivity**
  a · (b + c) = (a · b) + (a · c)
- **Identity**
  We call e an identity when e · a = a · e = a
  (usually denoted **0** for addition and **1** for multiplication operators)
- **Inverse**
  We call a^{-1} an inverse of a when $a^{-1} \cdot a = a \cdot a^{-1} = e$

Group

A group is an ordered pair (G, ·) where G is a set and · is a binary operation on G satisfying the following axioms:

- **Associativity**
- **Identity**
- **Inverse**
- **Closure**
  (For every a, b ∈ G, a · b is also in G)

Group order is the number of elements in G, while order of an element a from that group is a value n such that $a^n = e$.

Abelian group

A group is called abelian when its operator is **commutative**.

Cyclic group

A group that can be generated by repeatedly combining one of its elements with itself. We call that element the generator of the group.

Dihedral group

A set of symmetric transformations (rotations and flips) of a regular n-gon.
(Often denoted D_n)

Permutation group

A group (G, ·) is a permutation group when G is a set of bijective functions (permutations) from some set into itself and · operation is permutation composition. Its usually convenient to use cyclic notation to represent these permutations. For example a permutation taking elements (1,2,3,4,5) into (2,5,4,3,1) can be represented as (125)(34), while identity would be expressed as (1)(2)(3)(4)(5) or simply ().
(We usually omit writing 1-cycles)
A 2-cycle is called a transposition. Any permutation can be translated into a sequence of only transpositions (while omitting 1-cycles). Permutation group is called **even** if it translates into an even number of transpositions and **odd** otherwise.

Symmetric group

A permutation group consisting of all possible permutations on its permutation set M is symmetric.
(If M = {1,2,3,...,n} then we denote such a group as S_n)

Cosets

Let H ⊆ G, then for every x ∈ G:

$$xH = \{xh | h \in H\} \qquad Hx = \{hx | h \in H\}$$

are respectably left and right coset of H in G. Every coset in G is a subset of G.

Isomorphism

A group isomorphism from (G, ·) to (H, #) is a bijective mapping ψ : G → H such that for all u and v in G:

$$\psi(u \cdot v) = \psi(u) \,\#\, \psi(v)$$

Ring

A ring is a set R equipped with two binary operations + (addition) and · (multiplication) satisfying the following axioms:

- (R, +) is an **abelian** group
- **Multiplication associativity**
- **Addition and multiplication identities**
  (has **0** and **1**)
- **Distributivity**

Notation

Commutative ring

A ring with **commutative** multiplication.
($2\mathbb{Z}$, $3\mathbb{Z}$, $x\mathbb{Z}[x]$)

Division ring

A ring with **multiplication inverse**.
(Quaternions $\mathbb{H} = \{a + bi + cj + dk \,|\, a, b, c, d \in \mathbb{R}\}$)

Ideal

For and arbitrary ring (R, +, ·) a subset I is an ideal if:

- (I, +) is subgroup of (R, +)
- For every r ∈ R and x ∈ I, x · r ∈ I

Field

A field (F, +, ·) is a **commutative division ring** or, alternatively, a structure satisfying the following:

1. (F, +) and (F/{**0**}, ·) are **abelian** groups
2. **Distributivity**

($\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$)

Vector space

A vector space over a field (of scalars) F is a non-empty set V together with two binary operations that satisfy the *vector axioms*:

- (V, +) is an **abelian** group
- **Multiplicative identity**
  (1·**v**= **v**)
- **Vector distributivity**
  ($a\mathbf{u} + a\mathbf{v} = a(\mathbf{u} + \mathbf{v})$, $a\mathbf{v} + b\mathbf{v} = (a + b)\mathbf{v}$)
- a(b**v**) = (ab)**v**