Abstract Algebra

- Will only be looking at a very small subset of what this subject has to offer.
- Three main ideas here that need to be grasped:
  1. Group $\{G, \cdot\}$
  2. Ring $\{R_g, +, \times\}$
  3. Field $\{F, +, \times\}$
- Basically three different types of sets along with some operation(s).
- The classification of each set is determined by the axioms which it satisfies.

Group

- A **Group** $\{G, \cdot\}$ is a set under some operation $(\cdot)$ if it satisfies the following 4 axioms:

  1. **Closure** (A_1): For any two elements $a, b \in G$, $c = a \cdot b \in G$
  2. **Associativity** (A_2): For any three elements $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  3. **Identity** (A_3): There exists an **Identity** element $e \in G$ such that $\forall_{a \in G}$, $a \cdot e = e \cdot a = a$.
  4. **Inverse** (A_4): Each element in G has an inverse i.e. $\forall_{a \in G} \exists_{a^{-1} \in G}$, $a \cdot a^{-1} = a^{-1} \cdot a = e$.

- However it is said to be an **Abelian group** if in addition to the above the set follows the axiom:

   5. **Commutativity** (A_5): For any $a, b \in G$, $a \cdot b = b \cdot a$.

Cyclic group

- **Exponentiation** is repeated application of the group operator.
- We might have a^3 and this would equal $a \cdot a \cdot a$.
- So if the operation was addition then a^3 would in fact be $a + a + a$.
- Also we have $a^0 = e$ which for an additive group is 0.
- Also $a^{-n} = (a^{-1})^n$.
- A group is said to be **cyclic** if every element of the group G is a power a^k (where k is an integer) of a fixed element $a \in G$.

- The element a is said to generate G or be a **generator** of G.
- A cyclic group is always abelian and may be finite or infinite.
- If a group has a finite number of elements it is referred to as a **finite group**.
- The **order** of the group is equal to the number of elements in the group. Otherwise, the group is an **infinite group**.

Ring

- A binary operation is a mapping of two elements into one element under some operation. For a set S we have $f : S \times S \rightarrow S$.
- A **Ring** $\{R_g, +, \times\}$ is a set with two binary operations *addition* and *multiplication* that satisfies the following axioms:

  1. **Abelian Group under addition** $(A_1 \rightarrow A_5)$: It satisfies all of the axioms for an abelian group (all of the above) with the operation of *addition*. The identity element is 0 and the inverse is denoted $-a$.

2. **Closure under multiplication** (M_1): For any two elements $a, b \in R_g$, $c = ab \in R_g$.
3. **Associativity of multiplication** (M_2): For any elements $a, b, c \in R_g$, $(ab)c = a(bc)$.
4. **Distributive** (M_3): For any elements $a, b, c \in R_g$, $a(b + c) = ab + ac$.

- It is then said to be a **commutative ring** if in addition the ring follows the axiom:

5. **Commutativity** (M_4): For any $a, b \in R_g$, $ab = ba$.

- It is an **Integral domain** if in addition the commutative ring follows the axioms:

6. **Multiplicative Identity** (M_5): There is an element 1 in R_g such that, $a1 = 1a = a$ for all a in R_g.
7. **No Zero Divisors** (M_6): If $a, b \in R_g$ and $ab = 0$ then *either* $a = 0$ *or* $b = 0$.

- A **Field** $\{F, +, \times\}$ is a set with two binary operations *addition* and *multiplication* that satisfies the following axioms:
  1. **Integral Domain** $(A_1 - M_6)$: It satisfies all of the axioms for an Integral domain (all of the above).
  2. **Multiplicative Inverse** (M_7): Each element in F (except 0) has an inverse i.e., $\forall_{a \neq 0 \in F} \; \exists_{a^{-1} \in F}, \; aa^{-1} = a^{-1}a = 1.$
- In ordinary arithmetic it is possible to multiply both sides of an equation by the same value and still have the equality intact.

- Not necessarily true in finite arithmetic
- In this particular type of arithmetic we are dealing with a set containing a finite number of values.
- The set of real numbers is an infinite set and is not really useful for working with on computer systems due to the limited amount of memory and processing power.
- Much easier if every operation the computer performed resulted in a finite value that was easily handled. This is where finite fields come into play.

- Closure is the property that causes the result of a binary operation on an ordered pair of a set to be a part of that set also.
- The term *ordered pair* is important as it is not generally the case that $a \cdot b = b \cdot a$.

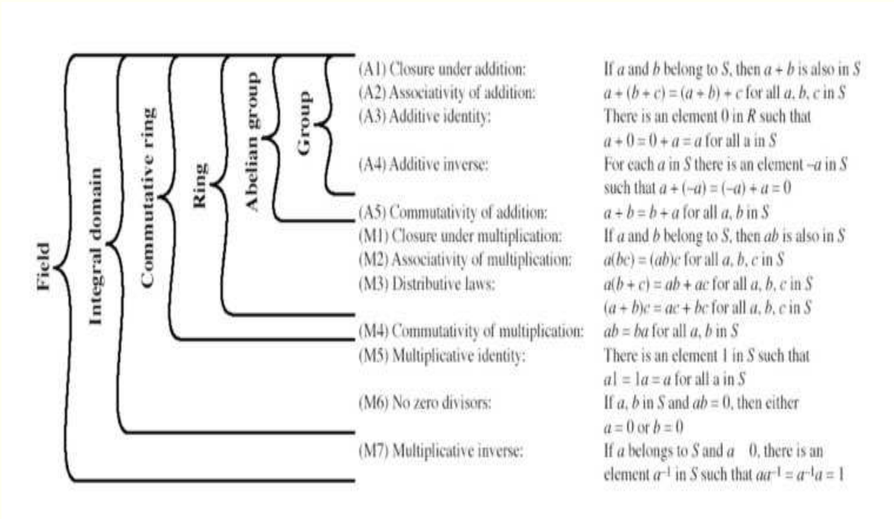

Figure 2: Group, Ring and Field