Groups & Fields

September 2, 2022

A **group** is a set G equipped with a binary operation $*$, satisfying the following four axioms.

1. **Closure:** $\forall g_1, g_2 \in G, g_1 * g_2 \in G$.
2. **Identity** $\exists g_0 \in G, \forall g \in G, g_0 * g = g * g_0 = g$. g_0 is called an identity element of the group.
3. **Inverses** $\forall g \in G, \exists g^{-1}, g * g^{-1} = g^{-1} * g = g_0$. Here g^{-1} is called the inverse element of g and g_0 is an identity element.
4. **Associativity** $\forall g_1, g_2, g_3 \in G, (g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$.

If an extra fifth condition:
$\forall g_1, g_2 \in G, g_1 * g_2 = g_2 * g_1$
is satisfied, the group is called an **Abelian group**.
Examples:

1. Integers under addition.
2. Non-singular real square matrices of fixed dimension under matrix multiplication

The first is an Abelian Groub, the second is a non-Abelian group.

A **field** is a set equipped with two operations addition (+) and multiplication (.), such that it forms an Abelian group under addition and an Abelian group under ., if in the second case, we exclude the additive identity element, 0.

Example: Integers modulo 5, with $+_5$ and $._5$ being addition and multiplication modulo 5.