Basic Notions of Groups and Fields

First, some notation: by $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}$ we mean the set of rationals, reals, integers and complexes, respectively. By $\mathbb{Q}^+, \mathbb{R}^+$ we mean positive elements of $\mathbb{Q}$ and $\mathbb{R}$ respectively.

Definition. *An **Abelian group** G is a set of objects together with an operation $\boxplus$ so that*

- *for every $x, y, z \in G$ we have $(x \boxplus y) \boxplus z = x \boxplus (y \boxplus z)$*
- *there exists an element $0 \in G$ so that $0 \boxplus x = x$ for every $x \in G$*
- *for every element $x \in G$ there exists an element $y \in G$ so that $x \boxplus y = 0$*
- *for every $x, y \in G$, we have $x \boxplus y = y \boxplus x$.*

Note: Sometimes, the identity is denoted by 1 instead of 0.
If $(G, \boxplus)$ has all but the last property, G is merely called a **group**.

Examples. *The following are examples of Abelian groups:*

(1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}$ *with regular addition.*
(2) *If $G = \{1, 2, 3, 4, 5\}$ and the operation $\boxplus$ is defined as $x \boxplus y = \min x, y$. Here, note G is finite.*

The following is a non-Abelian group:

(1) *If G is the set of $\mathbb{R}$ valued functions and $\boxplus$ is composition.*

The following are not examples of groups:

(1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}$ *with multiplication (why?).*
(2) *The positive reals with $x \boxplus y = x^y$ (why?).*

Definition. *A **field** F is a set of objects together with two operations $\boxplus, \boxdot$ so that the nonzero elements of F form an Abelian group under $\boxplus$ (with identity 0) and that the nonzero elements of F form an Abelian group under $\boxdot$. Furthermore, the following distributive law has to hold:*

$$x \boxdot (y \boxplus z) = x \boxdot y \boxplus x \boxdot z.$$

Examples. *The following are examples of fields:*

(1) $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ *with regular addition and multiplication.*
(2) $R^+, \mathbb{Q}^+$ *with regular addition and multiplication.*
(3) *For p a prime, the numbers $\{0, 1, 2, \ldots, p-1\}$ with $a \boxplus b = rem_p(a+b)$ and $a \boxdot b = rem_p(ab)$ (where $rem_p(x)$ is the remainder on dividing x by p). Here, note F is finite.*

The following are not fields:

(1) *The integers with regular addition and multiplication.*
(2) *For n composite, the numbers $\{0, 1, 2, \ldots, n-1\}$ with the same operations as in the finite field except we divide by n.*