CHAPTER I: FUNDAMENTALS

Section 4: Groups, Rings and Fields

In the previous sections we have seen several examples of sets of objects (numbers or functions mostly) that had an operation (or two) for which several properties are true. For example,

- In Section 1, we were introduced to S_n, the set of permutations of n objects under the operation of composition.
- In Section 2, we learned about $\mathbb{Z}_n$, the set of integers modulo n under the operations of modular addition and multiplication.
- In Section 3, we explored $\mathbb{R}[x]$, the set of polynomials with real coefficients (under addition and multiplication).

Also, in Section 3, we alluded to the notion of a field. In studying $\mathbb{R}[x]$, we noted that we didn't have to use $\mathbb{R}$, but any field would do. In this section, we'll define groups, rings and fields, and tie all of this together.

Definition: A ***group*** is a set G with an operation, denoted here by juxtaposition, such that the following properties are true:

(i) If $a,b,c \in G$, then $a(bc) = (ab)c$. (associativity)

(ii) There exists an element of G, call it e, such that for all $a \in G$, $ae = ea = a$. The element e is called the ***identity***.

(iii) For every $a \in G$, there exists an element $b \in G$ such that $ab = e$. The element b is called the ***inverse*** of a and is usually denoted by a^{-1}.

It needs to be noted that the way we have written this definition implies that the operation involved is multiplication, but this need not be the case. The operation could be composition, addition, multiplication, or any other operation defined on two objects. If the operation is addition, we could rewrite property (iii) as: There exists an element of G, call it 0, such that for all $a \in G$, $a + 0 = 0 + a = a$. Also, the notation for inverses certainly reminds us of multiplication, but in groups with addition, $a^{-1} = -a$. While the group axioms require that the operation be associative, we do not assume commutativity. If however, the operation is commutative, then the group is called ***abelian***.

Example 1: (a) S_n is a group under composition. The identity element is $e = (1)$.

(b) $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are all groups under addition. In fact, $\mathbb{Q}^*$ (the nonzero rational numbers) and $\mathbb{R}^*$ (the nonzero real numbers) are groups under multiplication as well.

(c) $\mathbb{C}$ is a group under complex addition and in fact under complex multiplication too.

(d) $\mathbb{Z}_n$ is a group under addition modulo n. The identity is 0.

(e) For prime p, $\mathbb{Z}_p^*$ is a group under multiplication modulo p. Since p is prime, these all have multiplicative inverses.

(f) $\mathbb{R}[x]$ is a group under addition of polynomials and if we leave out the zero polynomial, under multiplication too.

Note that we had to exclude 0 in order for $\mathbb{Q}$ and $\mathbb{R}$ to be groups under multiplication. The element 0 would never have a multiplicative inverse. Additionally, $\mathbb{Z}^*$ is not a group under multiplication since no integers would have inverses other than ± 1. Similarly, $\mathbb{Z}_n$ (where n is not prime) is not a group under multiplication modulo n. In this case some elements might have inverses, but as we saw in one of our homework problems some of the elements could be zero divisors as well.

So we have several examples of groups. But there are some clear differences between them. The set S_n only has one operation defined on it but $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ all have two operations. Every nonzero element in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$ has a multiplicative inverse, but most elements in $\mathbb{Z}$ do not. Most of these groups are abelian, but S_n is not. These differences are clarified with the following definitions.

Definition: A ***ring*** is a set R with two operations, generally called addition (denoted by $+$) and multiplication (denoted by juxtaposition) such that the following properties are true:

(i) R is an abelian group under addition.

(ii) Multiplication is associative.

(iii) The distributive law holds. Namely, for all $a, b, c \in R$, $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$.

Furthermore, multiplication need not be commutative, but if it is we

say R is a ***commutative ring***. There does not need to be a multiplicative identity, but if there is, we call it 1 and we say R is a ***ring with identity***. Finally, nonzero elements do not need to have inverses, but if R is a commutative ring with identity in which every nonzero element has an inverse, then we call R a ***field***.

Important note: the two operations defined on the set do not need to be addition and multiplication, however in general they are (for example in the sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$). Let's summarize all the possible properties a set can have and what the resulting object that satisfies those properties is called:

	Group	Abelian Group	Ring	Commutative Ring	Commutative Ring w/ identity	Field
Addition:						
associative	X	X	X	X	X	X
identity	X	X	X	X	X	X
inverses	X	X	X	X	X	X
commutative		X	X	X	X	X
Multiplication:						
associative			X	X	X	X
identity					X	X
inverses						X
commutative				X	X	X
Distributive Law			X	X	X	X

A group is the most basic and a field is the most complex. But in some ways fields are more familiar to us (since ordinary rational numbers and real numbers form fields).