Rings to Fields and the Necessity of These Terms

Shakeeb Uddin

Introduction

In the field of Abstract Algebra, where we focus on systems and structures of computation, we break down the understanding of our everyday arithmetic to make sense of it. There are certain type of structures that we use on a daily basis and those structures can be specified. In this paper, we will first dive into what a **ring** is, then we will look at **integral domains**, and finally take a look at **fields**.

However, one may question, what is the need of specifying that this group is a ring and this is an integral domain. In the text below, we will see what happens when the definition of a ring nor integral domain is given beforehand.

1 Rings

One of the first definitions that we will need is that of a ring.

Definition 1. A *ring* $(R, +, \cdot)$ comprises a set R and two binary operations $+, \cdot : R \times R \to R$, such that

1. $(R, +)$ is an abelian group (commutative). For all $a, b, c \in R$,
   (a) there is an identity element $0 \in R$ such that $a + 0 = 0 + a = a$.
   (b) for every $a \in R$, there is an additive inverse $-a \in R$ such that $a + (-a) = (-a) + a = 0$.
   (c) $a + (b + c) = (a + b) + c$.
   (d) $a + b = b + a$.
2. $(R, \cdot)$ is a monoid (associative and contains an identity element). For all $a, b, c \in R$,
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$
3. The multiplication operation $\cdot$ distributes over $+$, that is for all $a, b, c \in R$,
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ and}$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

[**?**]

This is the definition of a ring that will be found in most texts that are on the topic of Abstract Algebra. One thing to note about this definition is that we focus on the operation of $+$ more than we focus on the operation of $\cdot$. Every ring is a group.

Remark 1. There may be some discrepancies when reading other texts of Abstract Algebra. Most texts will only have three cases, while other will have four. The 4th one comes to be because most texts will omit mentioning the existence of a multiplicative identity element in R. However, we have covered this in our definition by mentioning that a ring is a monoid. A monoid is both associative and has an identity element [**?**].

An example of a ring would be the modulus integer structure $(\mathbb{Z}_m, +, \cdot)$.

Theorem 1. *For every $n \in \mathbb{N}, (\mathbb{Z}_n, +, \cdot)$ is a ring [**?**].*

Proof. The structure is already known to be an abelian group and $\cdot$ is associative on $\mathbb{Z}_n$. The first two conditions of a ring are already fulfilled. We are now able to focus on the distributive condition of a ring. Let $a, b, c \in \mathbb{Z}$. Then,

$$\begin{aligned} a \cdot (b + c) &= a(b + c) && \text{(by definition of multiplication in } \mathbb{Z}_n.) \\ &= (ab + ac) && \text{(by distributivity of } + \text{ and } \cdot \text{ in } \mathbb{Z}.) \\ &= ab + ac && \text{(by definition of addition in } \mathbb{Z}_n.) \\ &= a \cdot b + a \cdot c && \text{(by definition of multiplication in } \mathbb{Z}_n.) \end{aligned}$$

The proof of $(b + c) \cdot a$ is done within a similar manner. This concludes the proof. □

2 Integral Domains

Applying Definition **??**, we are now able to define what an integral domain is. Now that we know what a ring is **??**, we can now look at a specific type of ring.

Definition 2. Let $(R, +, \cdot)$ be a commutative ring (commutative with respect to $\cdot$).
R is an *integral domain* if and only if:

1. $0 \neq 1$.
2. R does not have any nonzero divisors.

[**?**]

Remark 2. Definition **??** is concise here because the Definition **??**. However, it may not always be the case that other texts will discuss a ring before an integral domain. Some works of Abstract Algebra might not even discuss a ring at all. If that is the case, the following may be used in which there are six conditions [**?**].

Definition 3. Let $(S, +, \cdot)$ be an algebraic system consists of two binary operations on S.
S is an *integral domain* if and only if:

1. Both operations are associative: for each $a, b, c \in S$,
$$a + (b + c) = (a + b) + c, \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c;$$
2. Both operations are commutative: for each $a, b \in S$,
$$a + b = b + a, \qquad a \cdot b = b \cdot a;$$
3. The operation $\cdot$ is distributive with respect to the $+$ operation: for each $a, b, c \in S$,
$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (b + c) \cdot a = b \cdot a + c \cdot a$$
4. There exists identity elements 0 and 1 in S relative to the operations $+$ and $\cdot$ respectively: for each $a \in S$,
$$a + 0 = 0 + a = a, \qquad a \cdot 1 = 1 \cdot a = a;$$

5. Each element $a \in S$ has an inverse $-a \in S$ relative to the operation $+$:

$$a + (-a) = (-a) + a = 0;$$

6. The cancellation law holds relative to the operation $\cdot$: for each $a, b, c \in S$,

$$\text{if} \quad a \cdot c = b \cdot c \quad \text{and} \quad c \neq 0, \quad \text{then} \quad a = b.$$

Theorem 2. *Let $(R, +, \cdot)$ be an integral domain, and $a, b, c \in R$ with $a \neq 0$. If $a \cdot b = a \cdot c$, then $b = c$, and if $b \cdot a = c \cdot a$, then $b = c$.*

[**?**]

Proof: Assume $a \neq 0$ and $a \cdot b = a \cdot c$. Then $a \cdot b - a \cdot c = 0$, so by distributivity, $a \cdot (b - c) = 0$. Since there are no divisors of zero in R and $a \neq 0$, $b - c = 0$. The proof of $b \cdot a = c \cdot a$ which implies $b = c$ is also done in a similar manner. □

3 Fields

Applying Definition **??** and Definition **??**, we are now able to define what a field is. As stated before, a field is a specification of something. An integral domain is a specific type of ring, and a field is a specific type of integral domain.

Definition 4 (Field)**.** The ring $(R, +, \cdot)$ is a *field* if and only if $(R, +, \cdot)$ is an integral domain and $(R - 0, \cdot)$ is an ablelian group.

[**?**]

Similar to the six conditions of an integral domain that was mentioned earlier **??**, in [**?**], they also give an informal and formal definition of a field. The informal definition was that a field was any structure that you could add, subtract, multiply, and divide. These types of structures act very close to the ones we use in everyday arithmetic.

In a more formal definition, the author states 12 tests that a structure must go through to be considered a field as cited within his text.

Definition 5. The following twelve test are to be referenced as the axioms for a *field*.

1. To any two elements a, b and the operation $+$, there corresponds a uniquely defined element c. We write $c = a + b$.
2. To any two elements a, b and the operation $\cdot$, there corresponds a uniquely defined element d. We write $d = a \cdot b$.
3. $a + b = b + a$, for all elements a, b.
4. $a \cdot b = b \cdot a$, for all elements a, b.
5. $a + (b + c) = (a + b) + c$ for all elements a, b, c.
6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all elements a, b, c.
7. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, for all elements a, b, c.
8. For any elements a and b, we can find one and only one element x such that $a + x = b$. We call this element $b - a$.
9. There is a unique element 0 such that $a + 0 = a$ for every element a.

10. For any elements a and b, provided only that a is not 0, there is one and only one element x such that $ax = b$. We call this element b/a.

11. There is a unique element 1 such that for every a, $a \cdot 1 = a$. The element 1 is not the same as the element 0.

12. $a \cdot b = 0$ only if $a = 0$ or $b = 0$.

[**?**]

Observe how many of these tests were already defined in Definition **??** and in Definition **??**. Rings and Integral Domains were not mentioned in this text at all, which led to the definition of a field being so long. If it had been the case that this definition of a field was used everywhere and rings and integral domains did not exist, then every structure that person would be given would have to go through 12 tests just to verify if the structure is in fact a field. However, by having these definitions, if a person was given a ring or integral domain and had to ascertain if it was a field, they would only have to verify a few more conditions.

If this was to be the case for other fields, then those terms that relied on other terms would have definitions that would go on for pages.

Conclusion

In this paper, we examined the definitions of a ring, an integral domain, and a field. We also observed what happens when one does not mention the previous definitions as well. The study of Abstract Algebra depends on building on what has been learned beforehand in order to build new topics. In such a way, we have not only proved of certain theorems relating to these structures, but also the need of these terms as well.