Abstract algebra

Introduction to rings and fields

Recall the group

A **group** $< A, * >$ is a set $A$ with a binary operation $*$ defined on $A$ that satisfies the four axioms below:

- $A$ is closed under $*$.
- The operation $*$ is associative.
- There is an identity element ($e$) in $A$.
- Each $x \in A$ has an inverse element $x' \in A$.

A group is a structure with one operation defined on it. As examples, we have considered the reals with the operation of addition (a group), and the the reals with the operation of multiplication (not a group, because the element 0 does not have a multiplicative inverse). The next step up is to look at a structure where two operations are defined on the set at once.

Ring

A **ring** $< A, +, * >$ is a set $A$ with two binary operations $+$ and $*$ defined on $A$ that satisfies the axioms below:

- $< A, + >$ is an Abelian group.

  An Abelian group is one that satisfies the commutative axiom under the operation: $a + b = b + a$ for all $a, b \in A$.

- $A$ is closed under $*$.
- The operation $*$ is associative.
- For all $a, b, c \in A$, the left distributive and right distributive laws hold:

  $$ a \ast (b + c) = a \ast b + a \ast c $$

  $$ (a + b) \ast c = a \ast c + b \ast c $$

The operations $+$ and $*$ are referred to as addition and multiplication, and in the context of real numbers, they are exactly what you think they are. Always keep in mind that when dealing with groups, rings, and fields at the abstract level, “addition” and “multiplication” may have other definitions.

This is a very brief intro to the idea of rings and fields - in this mini lecture, we won’t be considering any abstract examples. The main purpose here is to observe that the real numbers with addition and multiplication give the classic example of a ring.

$< \mathbb{R}, +, \ast >$
• \(< \mathbb{R}, + > \) (reals with addition) is an Abelian group.

• Multiplication \( (\ast) \) is associative and closed.

• Multiplication \( (\ast) \) distributes over addition \((+).\)

Note that while the reals must be a group under addition - closed, associative, additive identity \((0)\), additive inverse (negative) - the only requirement for multiplication is associativity (and closure)- we do not require a multiplicative identity or inverses as a defining property of a ring. Of course, the reals do have a multiplicative identity...

### Division ring

A ring with unity is a ring with a multiplicative identity \(1\):

\[1 \ast x = x \ast 1 = x \text{ for all } x \in A\]

An element \(u \in A\) is called a **unit** of \(< A, +, \ast >\) if it has a multiplicative inverse \(u' \in A\)

\[u \ast u' = u' \ast u\]

If every non-zero element of \(< A, +, \ast >\) is a unit, then \(< A, +, \ast >\) is a **division ring**.

So the reals with addition and multiplication are a division ring - every element except zero has a multiplicative inverse (reciprocal), which is what we need.

### Field

A **field** is a commutative division ring.

There, finally. That’s all we’re going for. What this boils down to is that the reals are (1) an Abelian group under addition, and (2) almost an Abelian group under multiplication. If you look at the properties picked up moving from ring to division ring to field, you see that you need multiplication to be associative and commutative, and for there to be a multiplicative identity, and multiplicative inverses for every element except the zero element. Furthermore, we require that multiplication distribute over addition.

So, think of the reals as the prototype- if we say that a set with addition and multiplication is a field, we’re saying it behaves in all the ways that we’d expect it to behave, based on our experiences with real numbers.

The things we need to look out for are the set-operation combinations that aren’t fields. If you’re familiar with matrices, that’s the best example to call to mind - the set of (say 2 by 2) matrices forms a group with addition, and a ring with addition and multiplication, but not a field: matrix-matrix multiplication is not commutative, and not all 2 by 2 matrices have multiplicative inverses.

The reals are an example of an **ordered field**. The field properties shown in the lecture, along with the ordering property and a couple others, are given on a separate reference sheet.

Proceed to reference sheet of reals properties.