

Math 412. Adventure sheet on operations and the definition of rings

DEFINITION: An **operation** on a set S is a function from $S \times S$ to S .


For example, addition and subtraction are operations on set the of integers (or on the set of real numbers). We might write \star for an operation, and write $x \star y$ to indicate the result of applying an operation to (x, y) , just as we would with the symbols $+$, $-$, etc.


A **ring** is a set with two operations, which we usually call addition and multiplication, that behave in similar ways to addition and multiplication of numbers. To make this precise, we specify some special abstract properties of operations.


- *Commutativity.* An operation \star is **commutative** if $x \star y = y \star x$ for any $x, y \in S$.
 - Find an example of an operation on the set of 2×2 matrices that *is* commutative, and an example of an operation on the same set that *is not* commutative. Can you think of more than one of each?
- *Associativity.* By definition, operations only take two inputs. If we wanted to operate on three things, we would have to choose two to pair first, then throw in the third. An operation \star is **associative** if we get the same result with either grouping: $(x \star y) \star z = x \star (y \star z)$ for any x, y, z in S .
 - Find an example of an operation on \mathbb{Z} that *is* associative, and an example of an operation on \mathbb{Z} that *is not* associative.
 - Let S be the set of functions $X \rightarrow X$ for some other set X . Prove that the operation on S “composition of functions” is associative.
 - Can you find an example of an operation on a set that *is* associative but *is not* commutative? What about the other way around? ¹
- *Identity.* An element $e \in S$ is an **identity** for \star if $e \star x = x \star e = x$ for all $x \in S$.
 - Which of the following operations have an identity? If so, what is it:
 - * addition on the set $\mathbb{R}[x]$ of real polynomials
 - * subtraction on the set $\mathbb{R}[x]$ of real polynomials
 - * multiplication of 2×2 matrices
 - * division of positive real numbers
 - * composition of functions
 - * averaging two rational numbers
 - * maximum of two rational numbers
 - Prove that any operation has at most one identity.
- *Inverses.* If \star is an operation with an identity e , then an **inverse** for an element x is another element y such that $x \star y = y \star x = e$.
 - For each of the operations above that has an identity, does it have an inverse? How do you find inverses for your operation?


¹Hint: Maybe something on the list of operations under “identity” works.

We can also describe operations by tables, like we do with $+$ tables and \times tables. Here are some operation tables for operations on the set $\{a, b, c, d\}$: the entry in row x and column y for operation \star means $x \star y$. Decide for each whether the operation is commutative, has an identity, and/or has inverses.

	a	b	c	d
a	a	b	c	d
b	b	b	c	d
c	c	c	c	d
d	d	d	d	d

	a	b	c	d
a	a	d	c	b
b	b	a	d	c
c	c	b	a	d
d	d	c	b	a

	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	a	c
d	a	d	c	b

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Bonus: Can you find natural operations on $\mathbb{Z}/4$ that correspond to some of these tables?

DEFINITION: A *ring* is a set R with two operations, denoted “+” and “ \times ” such that

- $+$ and \times are both associative,
- $+$ is commutative,
- $+$ has a identity, which we denote 0,
- Every element of R has an inverse for the operation $+$,
- \times has an identity², which we denote 1,
- The two operations are related by the *distributive properties*: $a \times (b + c) = a \times b + a \times c$ and $(a + b) \times c = a \times c + b \times c$.

A FEW RINGS:

- What does it mean to say that \mathbb{Z} is a ring? Is this true? Don’t prove your answer.
- What does it mean to say that \mathbb{Z}_N is a ring? Is this true? How would you prove it?
- Can you find a pair of operations from the tables above that make $\{a, b, c, d\}$ into a ring? Is there only one answer?

²WARNING: Our definition of ring differs from that of the text! Whenever we say ring, we mean a “ring with identity” in the notation of the book.