Rings and fields.

Renzo's math 366

1 Definitions

1.1 Operations

A **(binary) operation** on a set X is a function from $\star : X \times X \to X$. It is common to denote the element $\star((x, y))$ as $x \star y$.

An operation $\star$ is:

associative if for every $x, y, z \in X$

$$x \star (y \star z) = (x \star y) \star z.$$

commutative if for every $x, y \in X$

$$x \star y = y \star x$$

An element $e \in X$ is called an **identity** for $\star$ if for every $x \in X$

$$e \star x = x \star e = x.$$

Given an element $x \in X$, if there exists an element $y \in X$ such that:

$$x \star y = y \star x = e,$$

then y is called the **inverse** of x with respect to the operation $\star$.

Problem 1. *Show that usual addition is an operation on the set of integers. It is associative, commutative. It has an identity and every element has an inverse.*
Show that usual multiplication is an operation on the set of integers. It is associative, commutative. It has an identity but NOT every element has an inverse. Which integers admit an invers with respect to multiplication?

Now we generalize the structure that integers have to the notion of a ring.

1.2 Rings

A **ring** $(R, +, \cdot)$ consists of a set R plus two operations:

addition: is an associative, commutative operation. There is an identity element denoted 0, and every element r has an additive inverse, denoted $-r$.

multiplication: is an associative, not necessarily commutative, operation. There is an identity element, denoted 1. It is not required for a nonzero element to have a multiplicative inverse.

Further, addition and multiplication must satisfy the distributive laws: for any three elements $r_1, r_2, r_3 \in R$:

D1:

$$(r_1 + r_2)r_3 = r_1r_3 + r_2r_3$$

D2:

$$r_3(r_1 + r_2) = r_3r_1 + r_3r_2$$

A **field** $(K, +, \cdot)$ is a ring where multiplication is commutative and every element different from 0 has a multiplicative inverse.

2 Examples

2.1 Rational numbers

Show that the set of rational numbers $\mathbb{Q}$ with the usual operations of addition and multiplication is a field.

2.2 Polynomials

Let $\mathbb{R}[x]$ denote the set of polynomials in one variable with real coefficients. An element of $\mathbb{R}[x]$ is an expression of the form:

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0,$$

where all the a_i's are real numbers.

We define two operations as follows:

addition: if $p(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, q(x) = b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0$, then

$$p(x)+q(x) := (a_n+b_n)x^n+(a_{n-1}+b_{n-1})x^{n-1}+\ldots+(a_1+b_1)x+(a_0+b_0)$$

multiplication: we define multiplication for special polynomials called monomials. If $p(x) = a_n x^n$ and $q(x) = b_m x^m$, then

$$p(x)q(x) = (a_n b_m)x^{n+m}$$

1. Show that you can now define multiplication for arbitrary polynomials by imposing the distributive law.
2. Check that $\mathbb{R}[x]$ is a ring but not a field.
3. What are the elements of $\mathbb{R}[x]$ that admit a multiplicative inverse?

2.3 Matrices

Let $M(2, \mathbb{R})$ be the set of 2×2 matrices with real entries. An element of $M(2, \mathbb{R})$ has the form:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

where all the a_{ij} are real numbers.

We define one addition and two multiplication operations as follows. if $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, and $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$, then:

addition:

$$A + B := \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{bmatrix},$$

multiplication 1:

$$A \star B := \begin{bmatrix} a_{11}b_{11} & a_{12}b_{12} \\ a_{21}b_{21} & a_{22}b_{22} \end{bmatrix},$$

multiplication 2:

$$AB := \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{bmatrix},$$

1. Is $M(2, \mathbb{R})$ with addition and multiplication 1 a ring? Is it a field?
2. Is $M(2, \mathbb{R})$ with addition and multiplication 2 a ring? Is it a field?
3. What is the biggest difference you notice between the two ring structures?
4. In both cases, what are the elements that admit a multiplicative inverse?

2.4 Functions

Let $\mathcal{C}([0,1])$ denote the set of real valued continuous functions from the closed interval $[0,1]$. An element of $\mathcal{C}([0,1])$ is denoted $f : [0,1] \to \mathbb{R}$, or by $f(x)$ or just f.

We define the operation of addition and multiplication of functions just like in calculus, by

$$f + g(x) := f(x) + g(x)$$

$$fg(x) := f(x)g(x)$$

1. Is $\mathcal{C}([0,1])$ with the operation defined above a ring? Is it a field?
2. What elements in $\mathcal{C}([0,1])$ admit a multiplicative inverse?

2.5 $\mathbb{Z}/n\mathbb{Z}$

For every n, consider the set

$$\mathbb{Z}/n\mathbb{Z} := \{0, 1, \ldots, n\}$$

Show that you can define an addition and a multiplication operations that are very similar to the usual operations on integers and make $\mathbb{Z}/n\mathbb{Z}$ into a ring.

3 Functions of Rings

If we have two rings R_1 and R_2, then we are interested in studying the functions that "behave well", with respect to the operations. We formalize this concept with the following definition.

3.1 Homomorphism

A **homomorphism** of rings is a function

$$f : (R_1, +_1, \cdot_1) \to (R_2, +_2, \cdot_2)$$

such that for every $x, y \in R_1$:

- $$f(x_1 +_1 x_2) = f(x_1) +_2 f(x_2)$$
- $$f(x_1 \cdot_1 x_2) = f(x_1) \cdot_2 f(x_2)$$

A bijective ring homomorphism is called an **isomorphism**.

Problem 2. *1. What constant function is always (and rather stupidly) a ring homomorphism?*

2. What are all ring homomorphisms from the ring of integers to the ring of integers? Which of them are isomorphisms?

3. Show that if you think of $\mathbb{Z}/n\mathbb{Z}$ as a quotient set via the appropriate equivalence relation, then the projection function is a ring homomorphism.

4. Show that the evaluation function at any point is a ring homomorphism from $\mathbb{R}[x]$ to $\mathbb{R}$.

5. Is determinant a ring homomorphism from the ring of 2×2 matrices to $\mathbb{R}$?

4 Challenge: what is This?

Define the following equivalence relation on the set of polynomials $\mathbb{R}[x]$:

$$p(x) \sim q(x) \text{ if } \ x^2 + 1 \text{ divides } q(x) - p(x)$$

1. Check that this equivalence relation is compatible with both operations on polynomials. That means if $p_1 \sim p_2$ and $q_1 \sim q_2$, then

$$p_1 + q_1 \sim p_2 + q_2$$

$$p_1 q_1 \sim p_2 q_2$$

2. Check that the quotient set inherits a ring structure. Is it a field?

3. Write down some polynomials that live in the equivalence class of 0, of 1 and of -1.

4. Does this quotient remind you of something? Can you find a ring (or field) isomorphism with some familiar ring (or field)?