Projects 2: rings and fields.

Renzo's math 281

Instructions

Below you find a list of projects, whose goal is to explore some examples of rings and fields. You will be working in groups. Each group will be assigned a project. You will spend two hours in class working on the projects. Then:

1. *Each group will have 30 minutes to present some of your work.* ***Notice:*** *it is not necessary that the representative presents ALL that you have done. And it shouldn't be like... "go, go, go" until you run out of time: the group should select topics to design an effective 30 minute delivery of the essence of the work done.*

2. *Each group will write up (much much preferably using a computer) the work done (all of it). This document will be graded and compiled into a booklet that will be made available to everybody!*

Basic definitions

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 $-r$. In other words, $(R, +)$ is a group.

multiplication: is an associative, not necessarily commutative, operation. There is an identity element, denoted 1. It is not required for a non-zero 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** $(K, +, \cdot)$ consists of a set R plus two operations:

addition: is an associative, commutative operation. There is an identity element denoted 0, and every element k has an additive inverse, denoted $-k$. In other words, $(K, +)$ is a group.

multiplication: is an associative, commutative, operation. There is an identity element, denoted 1. Any non-zero element k must have a multiplicative inverse, denoted either k^{-1} or $1/k$. In other words, $(K - \{0\}, \cdot)$ is a group.

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:

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

Note: A field is always a ring, whereas a ring is not necessarily a field. Some example we know:

1. $\mathbb{Z}$ is a ring, but NOT a field.
2. $\mathbb{Z}/n\mathbb{Z}$ is a ring for all n. It is a field if and only if p is prime.
3. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, and therefore, also rings.

1 Group 1: 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 $p(x) = a_nx^n$ and $q(x) = b_mx^m$, then

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

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?
4. Define the notion of subring. Are the following subsets of $\mathbb{R}[x]$ subrings?
   - $\mathbb{R}^{\leq 2}[x]$:=polynomials of degree lower than or equal to 2 (i.e. $a_2x^2 + a_1x + a_0$);
   - $\mathbb{R}^{even}[x]$:= even polynomials (i.e. $a_{2m}x^{2m} + a_{2m-2}x^{2m-2} + \ldots + a_2x^2 + a_0$);

2 Group 2: 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?

3 Group 3: 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
3. Let $X_{3,0}$ be the set of functions that vanish at 3. ($X_{3,0} := \{f : f(3) = 0\}$). Is it a subring of $\mathcal{C}([0,1])$?
4. Let $X_{0,3}$ be the set of functions that have value 3 at 0. ($X_{0,3} := \{f : f(0) = 3\}$). Is it a subring of $\mathcal{C}([0,1])$?

4 Group 4: 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

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

$$p_1q_1\sim p_2q_2$$

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)?