OLGA RADKO MATH CIRCLE: ADVANCED 3

JOAQUÍN MORAGA

Worksheet 5: Fields

In Mathematics, a *Field* is a set on which addition, multipication, substraction, and division are defined and behave as they do in the real numbers ($\mathbb{R}$) or rational numbers ($\mathbb{Q}$).

The following set of rules are called *Field axioms*. These are the rules that a set F with addition $+$ and multiplication $\times$ must satisfy to be called a Field.

Definition 1. Let F be a set with two binary operations $+$ and $\times$. The first is called *addition* and the second *multiplication*. We say that F is a *Field* if it satisfies the following conditions:

(1) *Associativity*: $a + (b + c) = (a + b) + c$ and $a \times (b \times c) = (a \times b) \times c$ for every $a, b, c \in F$.
(2) *Commutativity*: $a + b = b + a$ and $a \times b = b \times a$ for every $a, b \in F$.
(3) *Identity:* There exists $0 \in F$ for which $0 + a = a$ for every $a \in F$. There exists $1 \in F$ for which $1 \times a = a$ for every $a \in F$.
(4) *Additive inverses:* For every $a \in F$ there exists $b \in F$ for which $a + b = 0$. This element b is usually denoted by $-a$.
(5) *Multiplicative inverses:* For every $a \in F$, with $a \neq 0$ there exists $b \in F$ for which $ab = 1$. This element is usually denoted by $b = a^{-1}$.
(6) *Distributive* of addition over multiplication: For every $a, b, c \in F$, we have that $a \times (b + c) = a \times b + a \times c$.

Problem 4.0: Decide whether the following sets with addition and multiplication are Fields or not:

- The integer numbers $\mathbb{Z}$ with the usual addition and multiplication.
- The rational number $\mathbb{Q}$ with the usual addition and multiplication.
- The real numbers $\mathbb{R}$ with the usual addition and multiplication.
- The complex numbers $\mathbb{C}$ with the usal addition and muiltiplication.
- The set $\mathbb{Z}_2 := \{0, 1\}$ with addition and multiplication modulo 2.
- The set $\mathbb{Z}_5 := \{0, 1, 2, 3, 4\}$ with addition and multiplication modulo 5.
- The set $\mathbb{Z}_6 := \{0, 1, 2, 3, 4, 5\}$ with addition and multiplication modulo 6.
- The set $M_{2\times 2}(\mathbb{Z})$ of 2×2 matrices with integer entries.
- The set $M_{2\times 2}(\mathbb{Q})$ of 2×2 matrices with rational entries.
- The set $\mathbb{R}[x]$ of real polynomials with variable x.
- The quaternions with the usual addition and multiplication.

Solution 4.0:

Problem 4.1: For each $n \in \{2, 3, 4, 5\}$. Show that there exists a Field F that has exactly n elements.
Solution 4.1:

Definition 2. Let R be a set with addition $+$ and multiplication $\times$. Let $0 \in R$ be the identity element with respect to the addition $+$. We say that two elements a and b are *zero divisors* if neither of them are zero and $a \times b = 0$. For instance, in $\mathbb{Z}_4$, we have that $2 \times 2 = 0$. However, $2 \neq 0$. Then, the element 2 is a zero divisor in $\mathbb{Z}_4$.

Problem 4.2: Show that a Field $(F, +, \times)$ contains no zero divisors.
Conclude that if n is a composite number, then $\mathbb{Z}_n$ is not a field.
Show that if p is a prime number, then $\mathbb{Z}_p$ is a field.
Solution 4.2:

Problem 4.3: Let $(F, +, \times)$ be a field. Show that $(F, +)$ and $(F \setminus \{0\})$ are groups.
Solution 4.3:

Definition 3. Let $\mathbb{Q}$ be the field of rational numbers. Let μ be a m-root of unity, i.e., a complex number for which $\mu^m = 1$. For instance, the number (-1) is a 2-root of unity. Consider the set

$$\mathbb{Q}(\mu) := \{q_1 + q_2\mu + \cdots + q_{m-1}\mu^{m-1} \mid q_i \in \mathbb{Q}\}.$$

This set is called the *extension of* $\mathbb{Q}$ *by* μ. For instance, if we extend $\mathbb{Q}$ with the 2-root of unity -1, then we just get $\mathbb{Q}$. If we extend $\mathbb{Q}$ with the 4-root of unity i, then we get

$$\mathbb{Q}(i) := \{q_1 + iq_2 \mid q_1, q_2 \in \mathbb{Q}\}.$$

These are called *rational complex numbers.*

Problem 4.4: Show that a m-root of unity must have the form

$$\cos\left(\frac{2k\pi}{m}\right) + i\sin\left(\frac{2k\pi}{m}\right),$$

where k is some integer in $\{0, \ldots, m-1\}$.

Let $\mathbb{Q}$ be the field of rational numbers and μ be a m-root of unity. Explains whether **Solution 4.4:**

Definition 4. Let $(F, +, \times)$ be a field. Let $H \subset F$ be a subset that contains 0 and 1 such that H becomes a field when we restrict the addition $+$ and the multiplication $\times$ to it. In this case, we say that H is a *subfield* of F and we write $H \leqslant F$.

For instance, we have a sequence of subfields:

$$\mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}.$$

Problem 4.5: Find all the fields F for which we have a sequence of subfields $\mathbb{R} \leqslant F \leqslant \mathbb{C}$.
Can you find an infinite sequence of fields $\{F_i\}_{i\geq 0}$ for which $F_0 = \mathbb{Q}$, $F_i \leqslant F_{i+1}$, and each $F_i \leqslant \mathbb{R}$?

Problem 4.6: Consider the three polynomials:

$$p_1(x) = x^3 - x^2 - x + 1,$$
$$p_2(x) = x^3 + x^2 + x^1 + 1.$$
$$p_3(x) = x^3 + 3x^2 - 6x - 18.$$

For each polynomial p_i, find all the solutions of p_i in the field $\mathbb{Q}$, in the field $\mathbb{R}$, in the field $\mathbb{C}$, in the field F_5, and the field F_7.

Solution 4.6:

Definition 5. Let $(F, +, \times)$ and $(H, +, \times)$ be two fields. A *field homomorphism* is a function $\phi\colon F \to H$ that satisfies the following conditions:

- $\phi(a + b) = \phi(a) + \phi(b)$ for every $a, b \in F$.
- $\phi(ab) = \phi(a)\phi(b)$ for every $a, b \in F$.
- $\phi(1_F) = 1_H$, where 1_F is the multipicative identity of F and 1_H is the multiplicative identity of H.

In other words, a field homomorphism is a function between the fields that "respect" the structure of both fields.

Problem 4.7: Let $(F, +, \times)$ and $(H, +, \times)$ be two fields and $\phi\colon F \to H$ be a field homomorphism. Let 0_F be the additive identity of F. Analogously, let 0_H be the additive identity of H.
Show that $\phi(0_F) = 0_H$.
Write an example of a field homomorphism.
Show that if p and q are prime numbers, then there are no field homomorphism $\phi\colon \mathbb{Z}_p \to \mathbb{Z}_q$.
Solution 4.7:

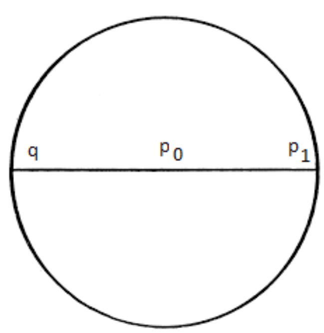
Definition 6. We say that two fields F and H are isomorphic if there exists a bijectivey field homomorphism between them.

Problem 4.8: Let $\mathbb{R}[x]$ be the set of real polynomials. We write $\mathbb{R}[x] \pmod{x^2+1}$ to be the set of real polynomials modulo the relation $x^2+1=0$. This means that in $\mathbb{R}[x] \pmod{x^2+1}$ two polynomials $p(x)$ and $q(x)$ are considered to be the same if $p(x)-q(x)$ is divisible by x^2+1.
Show that $\mathbb{R}[x] \pmod{x^2+1}$ is a field.
Show that $\mathbb{R}[x] \pmod{x^2+1}$ is isomorphic to $\mathbb{C}$.
Solution 4.8:

Definition 7. We consider an infinite ruler and a compass. The ruler is infinite however it has no measures, i.e., the ruler can only be used to draw finite line segments between two points in $\mathbb{R}^2$. The compass can only be used to draw a circle with center p and radius pq whenever p and q are two given points in the space $\mathbb{R}^2$. The compass does not have memory, i.e., it closes immediately after drawing the circle.

A *construction with ruler and compass* is a drawing that can be obtained using the "infinite ruler" and the "memoryless compass" starting from a single line segment of length 1 and endpoints p_0 and p_1.

For instance, an example of a construction with ruler and compass is a circle of radius 1. We can put the compass in the vertices p_0 and p_1 and draw the circle. Then, we can construct a segment of length 2. We can prolonge the line through p_0 and p_1 until we intersect the circle in a second point q. Then, the interval segment p_1q has length 2 as shown in the picture:



We say that a real number $x \in \mathbb{R}$ is *constructible* if starting with a line segment of length 1 we can draw a line segment of length x or length $-x$ via a construction of rules and compass.

Problem 4.9: Show that the integers are constructible real numbers.
Solution 4.9:

Problem 4.10: Show that if x is a constructible real number, then $\sqrt{x}$ is a constructible real number.
Solution 4.10:

Problem 4.11: Show that if x and y are constructible real numbers, then $x + y$ is a constructible real number. Show that if x and y are constructible real numbers, then $x \times y$ is a constructible real number.
Solution 4.11:

Problem 4.12: Show that if x is a non-zero constructible real number, then x^{-1} is a constructible real number.
Solution 4.12:

Problem 4.13: Let $\mathcal{C} \subset \mathbb{R}$ be the set of constructible real numbers.
Show that $\mathcal{C}$ with the usual addition and multiplication is a field.
Show that $\mathcal{C}$ is the smallest subfield of $\mathbb{R}$ that is closed under taking square roots of positive numbers.
Solution 4.13:

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555, USA.
Email address: jmoraga@math.ucla.edu