OLGA RADKO MATH CIRCLE: ADVANCED 3

JOAQUÍN MORAGA

Worksheet 6: Rings

In the previous weeks, we learnt about two objects: *Groups* and *Fields*.

Groups $(G, \times)$ have a single operation $\times$, a neutral element 1_G, and every element on G admits an inverse for $\times$. The most important groups that we learnt about are the groups of symmetries of geometric objects.

Fields $(F, +, \times)$, on the other hand, have two operations, both operations have neutral elements 0_F and 1_F, both operations admit inverses, and they enjoy various associativity properties. Some fields that we learnt about are the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$.

Some History:

The concept of *groups* was introduced by the mathematician Evarist Galois. Evarist Galois was a french mathematician. In Paris, on a dark morning in 1832, Evarist Galois died fighting a duel for a woman he fell in love with. Evarist Galois died at the age of 20. The night before the duel, Galois wrote a letter to his best friend. This letter contained the theory that made him immortal, the *Théorie des Groupes*. *Group Theory*, in English. However, he didn't enjoy success while alive. Galois got rejected three times by the top mathematics schools in France, after which he stopped trying. He sent his theories to famous mathematicians before dying. The first time, the mathematician lost his letters. The second time, the mathematician died before start reading it. 11 years after his death, his letters reach the hands of Joseph Liouville. Liouville convinced many mathematicians that the *Galois Theory* was revolutionary. Nowadays, Galois Theory is taught as a class in every single math major around the world and is an active research topic.

The concept of *fields* was introduced by Richard Dedekind in the mid-1800s. It is quite a much newer concept than the one of groups that was around in the early 1800s. Richard was a German mathematician. He wanted to introduce a term that mimics the definitions of rational numbers, real numbers, and complex numbers. He came up with the *field axioms* and called it a *Zählenkorper* which means *body of numbers*. In some way, he wanted to call these objects *bodies of numbers* because they "stay together" after we apply certain operations. Eliakim Moore was the first English-speaker mathematician who coined the concept *field*. Moore was the first head of the Mathematics Department at the University of Chicago, when it opened its doors in 1892. It is unclear why Moore chose the term *field*. In many other countries, the word *körper* is used. In France, fields are called *corps* while in Spain and Portugal fields are called *cuerpos*. Maybe, Moore did not want to use this term as it could resemble a human body, and of course, a field has nothing to do with that. *Field Theory* is also a class in every single math major around the world and is an active research topic.

Today, we will start discussing a different kind of algebraic objects. These objects are called *Rings*. Rings somehow sit in between groups and fields. They have as many operations (two) as fields but they may not have multiplicative inverses. At this point, you may be wondering: where does the name *ring* come from? We will give the answer below!

Definition 1. A ring $(R, +, \times)$ is a set R with two binary operations $+$ and $\times$ satisfying the following conditions (also called *ring axioms*):

(1) *Addition is associative:* For every $a, b, c \in R$, we have that $(a + b) + c = a + (b + c)$,
(2) *Addition is commutative:* For every $a, b \in R$, we have that $a + b = b + a$,
(3) *Additive identity:* There exists an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$,
(4) *Additive inverse:* For every $a \in R$ there exists an element $b \in R$ for which $a + b = 0$,
(5) *Multiplicative identity:* There exists an element $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$,
(6) *Mutiplicative associativity:* For every $a, b, c \in R$, we have that $a \times (b \times c) = (a \times b) \times c$, and
(7) *Left and righ distributivity:* For every $a, b, c \in R$, we have that $a \times (b + c) = a \times b + a \times c$ and $(a + b) \times c = a \times c + b \times c$.

The integer numbers $\mathbb{Z}$ with the usual addition and multiplication forms a ring. The identity for multiplication is $1 \in \mathbb{Z}$ and the identity for addition is $0 \in \mathbb{Z}$.

Definition 2. Let F be a field. For instance, you can think about the rationals $\mathbb{Q}$, reals $\mathbb{R}$, or complex numbers $\mathbb{C}$. We write $F[x]$ for the *polynomial ring over F with variable x*. The set $F[x]$ contains polynomials whose coefficients are in the field F. Every element $p(x)$ of $F[x]$ can be written uniquely as:

$$p(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n, \tag{0.1}$$

where the elements f_i belong to F and f_n is not zero. In the previous expression, the elements f_i are called the *coefficients* of $p(x)$ while the positive integer n is called the *degree* of the polynomial $p(x)$. We denote the degree of $p(x)$ by $\deg(p(x))$.

A polynomial is said to be *monic* if $f_n = 1$. For instance, $x^2 + 1$ is monic, but $3x^2 + 1$ is not monic.

For instance, the polynomial

$$\pi x^2 + 3$$

is an element of $\mathbb{R}[x]$. However, it is not an element of $\mathbb{Q}[x]$ as π is not a rational number. The function

$$\pi x^2 + \sin(x)$$

is not an element of $\mathbb{R}[x]$ as $\sin(x)$ is not a polynomial function.

We can use sum notation to write a polynomial as

$$p(x) = \sum_{i=0}^{n} f_i x^i. \tag{0.2}$$

The previous symbol, means that we are summing the expression $f_i x^i$ for all the possible values of i between 0 and n. Thus, the expression (0.2) and 0.1 are exactly the same. We may call (0.2) the abbreviated expression for the polynomial.

Problem 4.0: Consider the set $F[x]$ where F is a field. Let $p(x) = \sum_{i=0}^{n} f_i x^i$ and $q(x) = \sum_{i=0}^{m} g_i x^i$. We define the addition of polynomials as:

$$(p+q)(x) = \sum_{i=1}^{m+n} (f_i + g_i) x^i,$$

where we choose $f_i = 0$ (resp. $g_i = 0$) if $i > n$ (resp. $i > m$). Show that $(F[x], +)$ is an abelian group.
What is the identity element?
Write down the addition of the following polynomials:

- $x^2 + 1$ and $x^3 - 1$,
- $x^2 + x + 1$ and $x^2 - x + 1$.

Solution 4.0:

Problem 4.1: Consider the set $F[x]$ where F is a field. Let $p(x) = \sum_{i=0}^{n} f_i x^i$ and $q(x) = \sum_{i=0}^{m} g_i x^i$. We define the multiplication of polynomials as:

$$(pq)(x) = \sum_{k \geq 0} \left(\sum_{i+j=k} f_i g_j \right) x^k.$$

Write down the multiplication of the following polynomials:

- $x^2 + 1$ and $x^3 - 1$,
- $x^2 + x + 1$ and $x^2 - x + 1$.

Solution 4.1:

Problem 4.2: Let F be a field. Let $F[x]$ be the polynomial ring over F. Show that $(F[x], +, \times)$ is a ring. What is the multiplicative identity for this ring?
Solution 4.2:

Definition 3. Let $(R, +, \times)$ be a ring. An element u in R is called a *unit* or *invertible* if we can find an element $v \in R$ for which

$$u \times v = v \times u = 1_R.$$

For instance, the element $-1 \in \mathbb{Z}$ is a unit. Indeed, we have that

$$-1 \times -1 = 1.$$

Problem 4.3: Find all the units of the ring $(\mathbb{Z}, +, \times)$.
Find all the units of the ring $(\mathbb{R}[x], +, \times)$.
Find all the units of the ring $(\mathbb{Q}[x], +, \times)$.
Solution 4.3:

Definition 4. In the integer numbers $\mathbb{Z}$ we have some very special numbers called prime numbers. These are numbers which are only divisible by 1, itself, or the additive inverse of these.

In a ring R we have a similar concept of "primeness". We say that an element $p \in R$ is a *prime element* if whenever we write

$$p = ab,$$

then either a or b is a unit.

Problem 4.4: Show that a prime element in $\mathbb{Z}$ is a prime number.
Show that the element $x^2 + 4$ is not a prime element in $\mathbb{C}[x]$.
Show that the element $x^2 + 4$ is a prime element in $\mathbb{R}[x]$.
Show that $x^3 - 1$ is not a prime element in $\mathbb{R}[x]$. What about $x^3 + 1$? Is it prime in $\mathbb{Q}[x]$?
Solution 4.4:

Definition 5. In the integer numbers $\mathbb{Z}$ we learnt how to divide. The division in the integers works as follows. We grab two integers n and m and we want to divide n by m. Then, we try to find two integers q and r satisfying:

$$n = mq + r,$$

where $|r| < |m|$. Here, the number q is called the *quotient* and the number r is called the *residue*.

For the elements of $F[x]$ we have a similarly defined division. Let $f(x)$ and $g(x)$ be two polynomials in $F[x]$. The division of $f(x)$ by $g(x)$ is an expression of the form:

$$f(x) = g(x)q(x) + r(x),$$

where either $r = 0$ or $\deg(r(x)) < \deg(g(x))$. We call $q(x)$ the *quotient polynomial* and $r(x)$ the *residue polynomial*. We say that $g(x)$ divides $f(x)$ if the residue of the division is zero.

Problem 4.5: Perform the division of $x^3 + x^2 + x + 1$ by $x - 1$.
Perform the division of $x^3 - 1$ by $x - 1$.
Perform the division of $x^2 + 2x + 1$ by $x + 1$.
Perform the division of $2x + 4$ by $3x - 6$.
Solution 4.5:

Definition 6. Let $p(x) \in F[x]$ be a polynomial. Write

$$p(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n.$$

Let $f \in F$ be an element in the field. The evaluation of the polynomial $p(x)$ at the element $f \in F$ is the element of F given by the expression:

$$p(f) = f_0 + f_1 f + f_2 f^2 + \cdots + f_n f^n.$$

An element $f \in F$ for which $p(f) = 0$ is called a *root* of the polynomial $p(x)$.

Problem 4.6: Let $p(x)$ be a polynomial of degree n. Show that the following statements are equivalent:

- the element $c \in F$ is a root of $p(x)$,
- we can write $p(x) = (x - c)q(x)$ for some polynomial q of degree $n - 1$,
- the polynomial $x - c$ divides $p(x)$.

Solution 4.6:

Definition 7. Let $p_1(x), \ldots, p_r(x)$ be r polynomials in $F[x]$. The *greatest common divisor* of the polynomials $p_1(x), \ldots, p_r(x)$ is the monic polynomial $f(x)$ of largest degree which divides each of the given polynomials. We also write gcd for the greatest common divisor, as we do for integer numbers.

Problem 4.7: Find the greatest common divisor among the following set of polynomials in $\mathbb{R}[x]$:

- the polynomials x^2+1, x^2-1, and x^2-2.
- The polynomials x^3-1, x^4-1, and x^5-1.
- The polynomials x^3+3x^2+3x+1 and x^2+2x+1.

Solution 4.7:

Definition 8. Let μ_m be an m-root of unity, i.e., a complex number for which the equation

$$\mu_m^m = 1$$

holds. We define the the ring $\mathbb{Z}[\mu_m]$ to be the set of complex numbers of the form

$$\{a_0 + a_1\mu_m + a_2\mu_m^2 + \dots a_{m-1}\mu_m^{m-1} \mid a_0, \dots, a_{m-1} \in \mathbb{Z}\}.$$

For instance, the element $i \in \mathbb{C}$ is a 4-root of unity. The ring $\mathbb{Z}[i]$ is called the *ring of complex numbers*. It contains all the complex numbers $a+bi$ for which a and b are integer numbers.

If $\sqrt{n}$ is a root of a positive integer, then we write $\mathbb{Z}[\sqrt{n}]$ for the set of real numbers of the form $a+b\sqrt{n}$ where both a and b are integers.

Problem 4.8: Let μ_m be an m-root of unity. Show that $\mathbb{Z}[\mu_m]$ is a ring. Explain how the addition and multiplication works in this ring.
What are its units?

Let n be a positive integer. Show that $\mathbb{Z}[\sqrt{n}]$ is a ring. Explain how the addition and multiplication works in this ring.
What are its units?
Solution 4.8:

Problem 4.9 Is 5 a prime element in $\mathbb{Z}[i]$?
Is 5 a prime element in $\mathbb{Z}[\sqrt{2}]$?
Solution 4.9:

Problem 4.10: Find 5 different prime elements in $\mathbb{Z}[\sqrt{2}]$.
Solution 4.10:

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