OLGA RADKO MATH CIRCLE: ADVANCED 3

FERNANDO FIGUEROA, ROHAN JOSHI, JOAQUÍN MORAGA, AND CALEB PARTIN

Worksheet 5: Rings I

A *ring* $(R, +, \times)$ is a set R with two (binary) operations $+$ and $\times$, satisfying the following axioms for any elements a, b and c in R:

(a) Addition is associative: $(a + b) + c = a + (b + c)$
(b) Multiplication is associative:$(a \times b) \times c = a \times (b \times c)$
(c) Addition is commutative: $a + b = b + a$
(d) There exists an additive identity (0): $a + 0 = a$
(e) There exists a multiplicative identity (1): $a \times 1 = 1 \times a = a$
(f) There exist additive inverses (-a): $a + (-a) = 0$
(g) Multiplication is distributive with respect to addition: $a \times (b+c) = a \times b + a \times c$ and $(b+c) \times a = b \times a + c \times a$

If furthermore multiplication is commutative, we say that $(R, +, \times)$ is a *commutative ring*

Remark: We will sometimes omit the $\times$ symbol in between a parenthesis and an element of the ring, or between parentheses.

Problem 5.0: Which of the following are rings?

- $\mathbb{Z}$, with the usual $+$ and $\times$
- The set of even numbers, with the usual $+$ and $\times$
- The set of odd numbers, with the usual $+$ and $\times$
- A field.

Solution 5.0:

Problem 5.1: Show that a ring can only have one additive identity. In other words show that if z has the property that $z + w = w$ and z' has the property that $z' + w = w$, for every w in the ring. Then we must have $z = z'$

Show that a ring can only have one multiplicative identity

Solution 5.1:

Example 1: If $(R, +_R, \times_R)$ and $(S, +_S, \times_S)$ are two rings, then we define the operations in the ring $R \times S$ as follows:

- Its elements are of the form (a, b) for any a in R and b in S.
- Addition is performed term by term, i.e. $(a, b) + (c, d) = (a +_R c, b +_S d)$.
- Multiplication is performed term by term i.e. $(a, b) \times (c, d) = (a \times_R c, b \times_S d)$.

Example 2: If R is a ring we can define the ring of polynomials $R[x]$. Whose elements are polynomials in one variable with coefficients in R. Addition is performed by adding up the coefficients of monomials of the same degree, while multiplication is performed by multiplying the coefficients in the field and adding up the degrees of the monomials x^i, respecting the distributive property.

Similarly we can defined rings of polynomials in more variable over any ring.

Problem 5.2: In $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ compute the following:

- $(1, 2) \times (2, 3)$
- $(0, 2) \times (3, 0)$

In $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}[x]$ expand the following expressions:

- $(1, 5)((2, 3)x + (3, 4)x^2)$
- $((2, 3)x + (3, 4)x^2)((2, 0)x + (1, 1))$
- $((2, 3)x + (1, 1))^2$

Solution 5.2:

Problem 5.3: What is the multiplicative identity of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$?

Verify that Example 1 and Example 2 are rings. Can any of these examples be a field?

Solution 5.3:

The *characteristic* of a ring R is the smallest positive number n such that

$$\underbrace{1+\ldots+1}_{n \text{ times}} = 0.$$

If no such n exists, then we say that the ring has characteristic zero.

Problem 5.4: Compute the characteristic of the following rings:

- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$?
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$?
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$?

Solution 5.4:

Problem 5.5: Show that a finite ring (i.e. a ring with finitely many elements) does not have characteristic zero. Give an example of a ring with infinitely many elements, that has positive characteristic.
Solution 5.5:

Problem 5.6:

Show that the characteristic of a field is a prime number.

Give an example of a ring with prime characteristic that is not a field.

Solution 5.6:

Remember that a non-zero element a is a zero-divisor if there exists some non-zero element b, such that $a \cdot b = 0$.

Problem 5.7: Show that a ring whose characteristic is a composite number, must have some zero-divisors. Can you find rings of any characteristic with zero-divisors?

Solution 5.7:

Let $(R, +, \times)$ be a ring. A subring of $(R, +, \times)$ is a ring $(Q, +_Q, \times_Q)$, where Q is a subset of R, the operations in Q are the restrictions of the operations in R and the multiplicative identity of Q is the multiplicative identity of R.

Problem 5.8: Let Q be a subring of R

- Show that the additive identity of Q is the same additive identity of R
- Show that $\mathbb{Z}/m\mathbb{Z}$ has no proper subrings.
- Show that no proper subring of $\mathbb{Q}$ is a field.

Solution 5.8:

Problem 5.9: Ler m and n be coprime numbers. What are all the possible subrings of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$?
Solution 5.9:

Problem 5.10: What are all the subrings of $\mathbb{F}_p \times \mathbb{F}_p$?
Solution 5.10:

Problem 5.11: Show that $\mathbb{Q}$ has infinitely many different subrings.
Solution 5.11:

UCLA Mathematics Department, Los Angeles, CA 90095-1555, USA.
Email address: `fzamora@math.princeton.edu`

UCLA Mathematics Department, Los Angeles, CA 90095-1555, USA.
Email address: `rohansjoshi@math.ucla.edu`

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

UCLA Mathematics Department, Los Angeles, CA 90095-1555, USA.
Email address: `ctpartin@math.ucla.edu`