OLGA RADKO MATH CIRCLE, WINTER 2024: ADVANCED 3

FERNANDO FIGUEROA AND JOAQUÍN MORAGA

Worksheet 6:

Throughout this worksheet $\mathbb{F}$ is a field.

Let $p(x)$ be a polynomial in $\mathbb{F}[x]$. We will define the elements of $\mathbb{F}[x]/(p(x))$ to be polynomials in $\mathbb{F}[x]$, where we declare two polynomials to be equal in $\mathbb{F}[x]/(p(x))$ if their difference is divisible by $p(x)$. In other words, two polynoials $r(x)$ and $s(x)$ are equal in $\mathbb{F}[x]/(p(x))$ if there exists a polynomial $q(x)$ in $\mathbb{F}[x]$, such that:

$$r(x) - s(x) = p(x)r(x).$$

Notice that this is similar to the construction of $\mathbb{Z}/n\mathbb{Z}$.

Problem 6.1:

Compute how many elements the following sets have:

(1) $\mathbb{F}_5[x]/(x)$
(2) $\mathbb{F}_2[x]/(x^2 + 1)$
(3) $\mathbb{F}_3[x]/(x^3 + 1)$

Solution 6.1:

Problem 6.2:

Let $p(x)$ be a polynomial in $\mathbb{F}_q[x]$ of degree d.

How many elements does the set $\mathbb{F}_q[x]/(p(x))$ have?

Solution 6.2:

Problem 6.3:

The set $\mathbb{F}[x]/(p(x))$ has a ring structure, since we can have a notion of addition and multiplication coming from those of polynomials.

Make a multiplication table for the elements in $\mathbb{F}_2[x]/(x^2+1)$ and another one for the elements in $\mathbb{F}_2[x]/(x^2)$, then compare them.

Solution 6.3:

Remember that a ring is a field if every non-zero element is invertible.

Problem 6.4:

Which of the following rings are fields?

(1) $\mathbb{F}_2[x]/(x^2)$
(2) $\mathbb{F}_2[x]/(x^2+1)$
(3) $\mathbb{F}_{19}[x]/(x)$
(4) $\mathbb{F}_3[x]/(x^2+1)$
(5) $\mathbb{F}_5[x]/(x^2+1)$

Solution 6.4:

Remember that a polynomial $p(x)$ in $\mathbb{F}[x]$ is called irreducible if there are no two polynomials $r(x), s(x)$ in $\mathbb{F}[x]$ of degree at least one, such that:

$$p(x) = r(x)s(x)$$

.

Problem 6.5:

Show that the ring $\mathbb{F}_q[x]/(p(x))$ is a field if and only if $p(x)$ is irreducible.

Hint: You might want to show that a finite ring is a finite field if and only if the product of any two non-zero elements is again non-zero.

Solution 6.5:

A polynomial is called monic if the coefficient of the leading term is 1.

Problem 6.6:

Show that in $\mathbb{F}_p[x]$ there exist irreducible monic polynomials of degree 2.

Solution 6.6:

Problem 6.7:

How many irreducible polynomials of degree 2 are there in $\mathbb{F}_p[x]$?

Solution 6.7:

Problem 6.8: Show that in $\mathbb{F}_p[x]$ there exist irreducible monic polynomials of degree 3.
How many irreducible polynomials of degree 3 are there in $\mathbb{F}_p[x]$?
Solution 6.8:

We can make the same construction for any other ring, i.e. we can define $R[x]/(p(x))$ in the same way for an arbitrary ring.

For the following exercise let $R := \mathbb{Z}/4\mathbb{Z}$ **Problem 6.9:**

How many elements do the following rings have?

(1) $R[x]/(2x)$
(2) $R[x]/(x^2)$
(3) $R[x]/(2x^2 + x)$

Solution 6.9:

Problem 6.10:

Le R be the ring $\mathbb{Z}/m\mathbb{Z}$

Let $p(x)$ be a polynomial of degree d in $R[x]$. Can you find a general formula for the number of elements of $R[x]/(p(x))$?

What if we impose the condition that $p(x)$ is monic?

Solution 6.10:

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

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