Math 320 April 23, 2020

Continue with Ch 5:

Last time: we defined

$$F[x]/(p(x))$$

congruence classes of $F[x]$ mod $p(x)$.

elements: congruence classes mod $p(x)$

If $\deg p(x) = n$ then every element of $F[x]/(p(x))$ is of the form

$$[r(x)]$$

where $\deg r(x) < n$ or $r(x) = 0_F$.

Today: define addition and mult. on $F[x]/(p(x))$ and will make it into a ring.

Consider the set $F[x]/(p(x))$.

Define addition and multiplication on this set by

$$[f(x)] + [g(x)] = [f(x) + g(x)]$$

$$[f(x)] \cdot [g(x)] = [f(x) \cdot g(x)]$$

(very similar to congruence classes of integers)

With these two operations, $F[x]/(p(x))$ is a commutative ring with identity $[1_F]$:

$$[f(x)] \cdot [1_F] = [f(x) \cdot 1_F] = [f(x)]$$

Ex: Consider $\mathbb{R}[x]/(x^2+1)$

$p(x)$

here $\deg x^2+1 = 2$. Therefore, every element of $\mathbb{R}[x]/(x^2+1)$ is of the form

$$[a+bx], \text{ where } a,b \in \mathbb{R}$$

For example, two elements of this ring are $[1+2x]$, $[3-4x]$.

Let's add and multiply these two classes!

$$[1+2x]+[3-4x] = [(1+2x)+(3-4x)]$$
$$= [4-2x]$$

(in general, addition of classes is straightforward)

$$[1+2x][3-4x] = [(1+2x)(3-4x)]$$
$$= [3-4x+6x-8x^2]$$
$$= [3+2x-8x^2]$$

As stated above, every element of $\mathbb{R}[x]/(x^2+1)$ can be written in the form $[a+bx]$, $a, b \in \mathbb{R}$.

So, we should be able to do that with $[3+2x-8x^2]$.

How to do this: use the fact that in $\mathbb{R}[x]/(x^2+1)$, $[x^2+1] = [0]$

$$\Rightarrow [x^2+1] = [x^2] + [1] = [0]$$

$$\Rightarrow [x^2] = [-1]$$

what this means: Replace the x^2 in $[3+2x-8x^2]$ with -1:

we get

$$[3+2x-8x^2] = [3+2x+8] = [11+2x]$$

$$\Rightarrow [1+2x][3-4x] = [11+2x]$$

In general, in $F[x]/(x^2-a)$, we have

$$[x^2-a] = [0_F] \Rightarrow [x^2] = [a]$$

In previous example, a was -1.

Let's consider $[a+bx], [c+dx] \in \mathbb{R}[x]/(x^2+1)$:

$$[a+bx]\cdot[c+dx] = [(a+bx)(c+dx)]$$

replace w/ -1

$$= [ac + (ad+bc)x + bdx^2]$$

$$= [(ac-bd) + (ad+bc)x]$$

rule for multiplying two elements of $\mathbb{R}[x]/(x^2+1)$

Note: $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Another example: consider $\mathbb{Z}_2[x]/\underset{p(x)}{(x^2+x)}$

Since $\deg x^2+x = 2$, every element of $\mathbb{Z}_2[x]/(x^2+x)$ can be written as

$$[a+bx], \quad a, b \in \mathbb{Z}_2.$$

So, $\mathbb{Z}_2[x]/(x^2+x)$ has only 4 elements:

$[0], [1], [x], [1+x]$

So, we can write a mult. table:

$\cdot$	$[0]$	$[1]$	$[x]$	$[1+x]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[1+x]$
$[x]$	$[0]$	$[x]$	$[x]$	$[0]$
$[1+x]$	$[0]$	$[1+x]$	$[0]$	$[1+x]$

To get the last 4 entries, use the fact that

$$[x^2+x] = [0]$$

in $\mathbb{Z}_2[x]/(x^2+x)$. So we have

$$[x^2+x] = [x^2] + [x] = [0]$$

$$\Rightarrow \boxed{[x^2] = [-x] = [x]}$$ replace any x^2 with x

Now, we complete the table:

1. $[x]\cdot[x] = [x^2] = [x]$

2. $[x][1+x] = [x(1+x)] = [x + x^2]$

$$= [x] + [x^2]$$

$$= [x] + [x]$$

$$= [x+x] = [2x] = [0]$$

3. $[1+x][x] = [0]$

4. $[1+x]^2 = [1+x][1+x]$

$$= [(1+x)^2]$$

$$= [1+2x+x^2]$$

$$= [1] + [2x] + [x^2]$$

$$= [1] + [0] + [x]$$

$$= \boxed{[1+x]}$$

Summary: to define a mult. rule in $F[x]/(p(x))$, use the rule

$$[p(x)] = [0_F]$$

to "reduce" the degrees of the terms