Math 320 April 28, 2020

final is take-home; have 4-5 days to complete; not collaborative

- cover 3.3, 4.1-4.5, 5.1-5.3, whatever we see in Ch 6
- lots of OH the Fri, weekend before finals week

Last time: computing addition and multiplication in $F[x]/(p(x))$.

Units in $F[x]/(p(x))$.

Question: when is $[f(x)] \in F[x]/(p(x))$

Thm 5.9: If $f(x) \in F[x]$ and $f(x)$, $p(x)$ are relatively (i.e. their gcd is 1_F) then $[f(x)]$ is a unit in $F[x]/(p(x))$.

Note the similarities with the integer version of this theorem: $[a]$ is a unit in $\mathbb{Z}_n$ if $(a,n)=1$.

Pf: Suppose $(f(x), p(x)) = 1_F$. Then, there exist $u(x), v(x) \in F[x]$ such that

$$f(x)\cdot u(x) + p(x)\cdot v(x) = 1_F$$

What is our goal? Show $[f(x)]$ is a unit. So, we need a $[g(x)]$ such that $[f(x)][g(x)] = [1_F]$.

We'll use the linear combo to accomplish this. Rearrange the linear combo a bit:

$$f(x)\cdot u(x) - 1_F = p(x)\cdot v(x)$$

$$\Rightarrow p(x) \mid (f(x)\cdot u(x) - 1_F)$$

$$\Rightarrow f(x)\cdot u(x) \equiv 1_F \mod p(x)$$

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

So, $[u(x)]$ is the (mult.) inverse of $[f(x)]$ in $F[x]/(p(x))$. ∎

Ex: consider $[x+2] \in \mathbb{Q}[x]/(x^2-9)$

($[x+2]$ = $f(x)$, (x^2-9) = $p(x)$)

- the factors of x^2-9 are $1, x-3, x+3$, and x^2-9.
- the factors of $x+2$ are 1 and $x+2$.

Therefore, $(x+2, x^2-9) = 1$, so by this theorem, $[x+2]$ is a unit in $\mathbb{Q}[x]/(x^2-9)$.

Note: to find the inverse of $[x+2]$, set up a linear combo

$$(x+2)u(x) + (x^2-9)v(x) = 1$$

where both $u(x)$, $v(x)$ are degree 1, so $u(x) = ax+b$, $v(x) = cx+d$.

then, solve this system of equations for a, b, c, d. Then, the inverse

of $[x+2]$ is $[ax+b]$.

See 5.2.14 for examples.

Section 5.3

Question: When is $F[x]/(p(x))$ a field?

Useful Theorem:

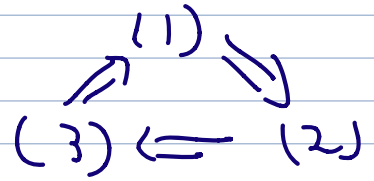
Thm 5.10: TFAE

(1) $p(x)$ is irreducible

(2) $F[x]/(p(x))$ is a field

(3) $F[x]/(p(x))$ is an integral domain.

Pf: We'll use the following structure:



(1) $\Rightarrow$ (2) "If $p(x)$ is irreducible, then $F[x]/(p(x))$ is a field."

We show every nonzero element of $F[x]/(p(x))$ is invertible.

Suppose $[f(x)] \in F[x]/(p(x))$ is nonzero.

If $[f(x)] \neq [0]$, then $p(x) \nmid f(x)$.

$p(x)$ is irreducible, so its only factors are of the form:

(i) c, $c \in F$ (constants) ← only possible common divisors

~~(ii) $c \cdot p(x)$, $c \in F$ (associates)~~

Since $p(x) \nmid f(x)$, the only common factors are constants, so $(f(x), p(x)) = 1_F$.

So, by Thm 5.9, $[f(x)]$ is a unit in $F[x]/(p(x))$

$[f(x)]$ is arbitrary, so this applies to every nonzero element of $F[x]/(p(x))$ $\Rightarrow$ it is a field.

(Note: (i) if $p(x) \mid f(x)$, then $p(x) \mid (f(x) - 0)$

So $f(x) \equiv 0 \mod p(x) \Rightarrow [f(x)] = [0]$

So if $[f(x)] \neq [0]$, then $p(x) \nmid f(x)$.

(ii) if an associate $cp(x) \mid f(x)$, then

$f(x) = c \cdot p(x) \cdot h(x)$ f.s. $h(x)$.

then $f(x) = p(x) \cdot \underbrace{(c \cdot h(x))}_{k(x)} = p(x) \cdot k(x)$

so $p(x) \mid f(x)$.

(2) $\Rightarrow$ (3) "If $F[x]/(p(x))$ is a field, then it's an integral domain."

Recall: in general, all fields are integral domains.

So this is automatically true.

(3) $\Rightarrow$ (1) "If $F[x]/(p(x))$ is an integral domain, then $p(x)$ is irreducible.

Recall: A subset D of a comm. ring R with identity if $\forall\, a, b$ such that $a \cdot b = 0_R$, either $a = 0_R$ or $b = 0_R$.

(same as no zero divisors)

Now we're assuming $F[x]/(p(x))$ has this property. Use this to show $p(x)$ is irreducible in $F[x]$.

Use the following fact (similar to prime #'s):

$p(x)$ is irreducible iff whenever $p(x) \mid b(x) \cdot c(x)$, either $p(x) \mid b(x)$ or $p(x) \mid c(x)$.

We'll start there: assume $p(x) \mid b(x) \cdot c(x)$

This means $b(x)\,c(x) \equiv 0_F \mod p(x)$.

$\Rightarrow$ $[b(x)\,c(x)] = [0_F]$ in $F[x]/(p(x))$

$\|$

$[b(x)] \cdot [c(x)]$

We have $[b(x)] \cdot [c(x)] = [0_F]$

Since $F[x]/(p(x))$ is an integral domain, either $[b(x)] = [0_F]$ or $[c(x)] = [0_F]$

$\Rightarrow$ $b(x) \equiv 0_F \mod p(x)$ or $c(x) \equiv 0_F \mod p(x)$

$\Rightarrow$ $p(x) \mid b(x)$ or $p(x) \mid c(x)$

$\Rightarrow$ $p(x)$ is irreducible in $F[x]$. ∎

What this theorem tells us: If you can show $p(x)$ is irreducible in $F[x]$, then you will have that $F[x]/(p(x))$ is a field.

So, if you're asked: "Is $F[x]/(p(x))$ a field?" all you need to do is check if $p(x)$ is irreducible.

Examples:

(1) Is $\mathbb{R}[x]/(x^2+1)$ a field?

check if x^2+1 is irreducible in $\mathbb{R}[x]$.

We know x^2+1 is irred. in $\mathbb{R}[x]$ (no real roots), so $\mathbb{R}[x]/(x^2+1)$ is a field

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

(2) $\mathbb{Q}[x]/(x^2-4)$ is this a field?

check if x^2-4 is irred. in $\mathbb{Q}[x]$.

it is <u>not</u> irreducible: $(x^2-4) = (x-2)(x+2)$

therefore, $\mathbb{Q}[x]/(x^2-4)$ is not a field.

It's not even an integral domain:

$$[x-2][x+2] = [(x-2)(x+2)] = [x^2-4] = [0]$$

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

(zero divisors)

This shows how to find zero divisors of $F[x]/(p(x))$: find two factors, $f(x), g(x)$ such that $f(x)\cdot g(x) = p(x)$.

Then, $[f(x)]\cdot[g(x)] = [p(x)] = [0_F]$

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

$([f(x)] = [0_F]$ if $p(x) \mid f(x))$

(3) Is $\mathbb{Q}[x]/(x^7 - 39x^5 + 52)$ a field?

By Eisenstein w/ $p = 13$, $x^7 - 39x^5 + 52$ is irreducible,

so $\mathbb{Q}[x]/(x^7 - 39x^5 + 52)$ is a field.

(4) $\mathbb{Z}_3[x]/(\underbrace{x^4 + x^3 + x^2 + 2}_{p(x)})$ is this a field?

no, 2 is a root of $p(x)$:

$p(2) = 16 + 8 + 4 + 2 = 30 = 0$ in $\mathbb{Z}_3$

so, by the Factor theorem, $(x-2) \mid p(x)$.

So $p(x)$ is reducible $\Rightarrow$ $\mathbb{Z}_3[x]/(x^4 + x^3 + x^2 + 2)$ not a field.

Since $x-2 \mid p(x)$, this tells us it's a zero divisor:

$p(x) = (x-2) \cdot h(x)$ s.t. $h(x) \in \mathbb{Z}_3[x]$

$\Rightarrow [x-2] \cdot [h(x)] = [p(x)] = [0]$

↑ ↗
zero divisors.

Note: zero divisors and roots are <u>not</u> the same

Chapter 6 : Ideals and Quotient Rings

Goal: develop notion of congruence for arbitrary rings.

integers ⟶ polynomials ⟶ arbitrary rings

$\mathbb{Z}_n$ ⟶ $F[x]/_{p(x)}$ ⟶ quotient rings

Past examples:

(1) $a \equiv b \mod 3$ means

$3 \mid (a-b)$ i.e. $a-b = 3k$ f.s. $k \in \mathbb{Z}$.

Let's consider the set

$$I = \{0, \pm 3, \pm 6, \ldots \pm 3k, \ldots\}$$

$$= \{3k : k \in \mathbb{Z}\}.$$

What we see: $a \equiv b \bmod 3$ if and only if $a - b \in I$.

Also, notice that I has the following "absorption" property:

if $n \in \mathbb{Z}$ and $m \in I$, then $nm = mn \in I$

$m = 3k$, and

$nm = 3(kn) \in I$.

(2) Similar example with polynomials:

"$f(x) \equiv g(x) \bmod x^3 - 2$ in $\mathbb{Q}[x]$"

means $x^3 - 2 \mid f(x) - g(x)$, so

$f(x) - g(x) = (x^3 - 2)k(x)$, for some $k(x) \in \mathbb{Q}[x]$

Consider the set

$$J = \{ k(x)(x^3 - 2) : k(x) \in \mathbb{Q}[x] \}$$

Similar to above: $f(x) \equiv g(x) \bmod x^3 - 2$ if and only if $f(x) - g(x) \in J$.

J also has the "absorption" property: if $r(x) \in F[x]$ and

$j(x) \in J$, then $r(x) \cdot j(x) \in J$:

$j(x) = (x^3 - 2) \cdot k(x)$ f.s. $k(x)$, so

$$r(x) \cdot j(x) = \big(r(x) \cdot k(x)\big)(x^3 - 2) \in J.$$

We're going to use these types of sets to define congruence for arbitrary ring:

★ Definition: A subset I of a ring R is called an <u>ideal</u> if

(1) $0_R \in I$

(2) I is closed under subtraction

(3) If $r \in R$ and $s \in I$, then both rs and $sr \in I$.