Math 320 May 7, 2020

- Will be office hours/review sessions on Sat + Sun.
- Also, you can email me to ask questions or set up a meeting.

Today: final prep

final: 8 questions + Extra Credit

Have from Sunday evening until 11:59 pm on Friday.

Question 1: ring theory question (short)

Question 2: determine if certain rings are fields

Questions 3 + 4: polynomials (Ch 4)

Question 5: Isomorphism problem (3.3)

Question 6: Ideal question + Congruence

Question 7: difficult polynomials + irreducibility

Question 8: difficult but can be short.

Summary of what we've covered (3.3 - 6.1)

3.3 Isomorphisms and homomorphisms

- Showing two Rings are isomorphic
  - come up w/ function $f: R \to S$ that's injective, surjective, and a homomorphism
  - properties of homomorphisms (Thm 3.10)
- Showing when rings are <u>not</u> isomorphic.
  - to do this, show that the two rings (call them R and S) have different "structural properties"
    - Examples:
      - cardinality: if $|R| \neq |S|$ then $R \not\cong S$
      - commutativity
      - # of zero divisors and or units
      - are both rings fields? integral domains?
      - characteristic

Ch 4 Polynomials

- Divisibility, GCDs (linear combos)
  - if $d(x) = \gcd(f(x), g(x))$, then
    $\exists$ polys $u(x), v(x)$ s.t.

$$f(x)\cdot u(x) + g(x)\, v(x) = d(x).$$

  - note: converse is <u>not</u> true unless $d(x) = 1_F$.

- Degree of a polynomial. Useful formula:

★ If $f(x) = g(x)\,h(x)$, then

$$\deg f(x) = \deg[g(x)\,h(x)] = \deg g(x) + \deg h(x)$$

- Roots, Factor Theorem
- Reducibility, Irreducibility.
  - A poly $f(x) \in F[x]$ is <u>reducible</u> if $\exists\ g(x), h(x) \in F[x]$ such that

$$f(x) = g(x)\,h(x)$$

and $g(x), h(x)$ are nonconstant polys of lower degree than $f(x)$.

  - A poly $p(x) \in F[x]$ if it <u>cannot</u> be factored into nonconstants of lower degree.

- another way to say this: $p(x)$ is irreducible if its only factors are constants and associates.

- How to show a polynomial is irreducible:
  - Useful fact: $p(x)$ is irreducible if and only if whenever $p(x) \mid b(x) \cdot c(x)$, either $p(x) \mid b(x)$ or $p(x) \mid c(x)$.
  - Tools for showing irreducibility.
  - If $\deg f(x) = 2$ or 3, then all you need to do is check for roots.
    - in this case, no roots $\Rightarrow$ irreducible
  - If $\deg f(x) \geq 4$, you should still check for roots, but then you <u>need</u> to do more.
  - For <u>any</u> polynomial, regardless of degree,
    - root $\Rightarrow$ reducible

Summary: - if deg 2 or 3, just check for roots
- if higher degree, still check for roots, but also do more.

- Another test for irreducibility: directly check for factors.

Ex: Show $f(x) = x^4 - 2x^2 + 8x + 1$ has no factors of degree 2 in $\mathbb{Q}[x]$.

To do this, suppose there exist factors $x^2 + ax + b$, $x^2 + cx + d$ (can assume $a, b, c, d \in \mathbb{Z}$)

$$x^4 - 2x^2 + 8x + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

Expand the right side. Then the coefficients on both sides of the equation should be the same. This sets up a system of equations. Show that this system has no solution, by getting two equations that contradict each other.

In summary to directly show a degree 4 polynomial $f(x)$ is irreducible:

(1) show $f(x)$ has no roots

(2) set up the above system of equations has no solution.

- did examples in class, on hw, in book

(Example 3 on page 115)

Note: don't have to do this if you can easily see that the polynomial is <u>reducible</u>

Ex: $x^4 + 4x^2 + 4 = (x^2 + 2)^2$

This same exact method works for polys with coefficients in $\mathbb{Z}_p$:

Ex: Show $g(x) = x^4 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

(1) Check for roots: we're in $\mathbb{Z}_2$, so only need to check 0 and 1:

$g(0) = 1$
$g(1) = 3 = 1.$ $\Rightarrow$ no roots

(2) Check for degree 2 factors:

$$x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d) \qquad (a, b, c, d \in \mathbb{Z}_2)$$

$$x^4 + x + 1 = x^4 + (a+c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd$$

$\Rightarrow$ $a + c = 0$, $ac + b + d = 0$, $ad + bc = 1$, $bd = 1$.

We can see that $b = d = 1$. (in $\mathbb{Z}_2$, $1 = -1$)

Then, $1 = ad + bc = a + c$

This contradicts $a + c = 0$.

This contradiction proves that such a factorization does not exist.

* One more useful tool you can use without proof: Let $f(x) \in F[x]$, $c \in F$.

If $f(x + c)$ is irreducible, then $f(x)$ is irreducible

Note: used in group work (7?):

Proved $f(x) = x^4 + 1$ is irreducible in $\mathbb{Q}[x]$ by showing that

$$f(x + 1) = (x + 1)^4 + 1 \text{ is irreducible}$$

This method works regardless of the coefficient field.

Next tools for irreducibility tools only work for proving irreducibility in $\mathbb{Q}[x]$.

(1) Rational Root Test: $f(x) = a_n x^n + \dots + a_1 x + a_0$ is a polynomial with integer coefficients

If $r, s \in \mathbb{Z}$ and r/s is a root of $f(x)$, then $r \mid a_0$, $s \mid a_n$.

Warning!! Do not use this test when the coefficients of $f(x)$ are in $\mathbb{Z}_p$.

(2) Eisenstein's Criterion: $f(x) = a_n x^n + \dots + a_1 x + a_0$ with integer coefficients. If there exists a prime p such that

$p \nmid a_n$, $p \mid a_{n-1}, a_{n-2}, \dots, a_0$, and $p^2 \nmid a_0$,

then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Warning!! only use for polys with integer coefficients.

(3) (Thm 4.25) Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with **integer coefficients**

Let p be a positive prime that doesn't divide a_n. Then, if the poly

$$[a_n]_p x^n + [a_{n-1}]_p x^{n-1} + \cdots + [a_1]_p x + [a_0]$$

is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Ex: Show that $f(x) = 3x^4 + 6x^3 + 16x^2 + 13x + 1$ is irreducible in $\mathbb{Q}[x]$.

Reduce the coefficients mod 2:

$$\bar{f}(x) = [3]_2 x^4 + [6]_2 x^3 + [16]_2 x^2 + [13]_2 x + [1]_2$$

$$\bar{f}(x) = x^4 + x + 1 \leftarrow \text{this is in } \mathbb{Z}_2[x].$$

We already showed that this poly is irreducible in $\mathbb{Z}_2[x]$.

So, since $\bar{f}(x) = x^4 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$, we conclude that $f(x) = 3x^4 + 6x^3 + 16x^2 + 13x + 1$ is irreducible in $\mathbb{Q}[x]$.

(See example 6 on page 118)

Partial example: Show that $2x^4 + 3x^3 + 6x + 6$ is irreducible in $\mathbb{Q}[x]$ using Thm 4.25.

To start, you can't reduce mod 2 since 2 divides the leading coefficient.

Then, you move on to $\mathbb{Z}_3$.

If the polynomial in $\mathbb{Z}_3$ is reducible in $\mathbb{Z}_3[x]$, then move on to $\mathbb{Z}_5[x]$ and so on...

Warning!! Thm 4.25 only works for polys with integer coefficients

Chapter 5: Congruence in $F[x]$.

- congruence mod $p(x)$; congruence classes.
- ring of congruence classes $F[x]/(p(x))$
- how to define addition and mult. in $F[x]/(p(x))$; understanding what elements of $F[x]/(p(x))$ look like.

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

★. $F[x]/(p(x))$ is a field if and only if $p(x)$ is irreducible in $F[x]$.

- If $p(x)$ is reducible, then $F[x]/(p(x))$ is not even an integral domain.
  - to find zero divisors, just look at the factors of $p(x)$.
  - Example: $\mathbb{Q}[x]/(x^2-4)$
    - $x^2-4 = (x-2)(x+2)$ so it's reducible
    $\Rightarrow \mathbb{Q}[x]/(x^2-4)$ is <u>not</u> a field
    - some zero divisors: $[x-2]$, $[x+2]$
    - Note: roots $\neq$ zero divisors.
  - So, if you want a field of the form $F[x]/(p(x))$, find poly $p(x)$ that's irreducible in $F[x]$.

Section 6.1:

- definition of an ideal
- Showing two ideals are equal (just some set theory)
- finitely generated ideals: (c), $(c_1, c_2, \dots, c_k)$
- congruence mod an ideal
  - if I is an ideal, then $a \equiv b \bmod I$ means $a - b \in I$.