Welcome back

We are all in this together and we will get through this together.

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 7.5–7.6; for Wed: 7.7.
- PS08: Outline due Wed, full version due Mon. (But deadlines are elastic.)

All plans are written in sand!!!

- Exam 2 (tentatively) on Wed Apr 22; done on paper, submitted by Canvas, proctored by Zoom.
- For Wed: Try to get some kind of camera (even phone) where I can see you all at the same time on Zoom.

Last: Principal ideal domains

Definition

To say that a ring R is a **principal ideal domain**, or **PID**, means that R is an integral domain (has the Zero Factor Property) and that every ideal of R is principal. I.e., second condition says that if I is an ideal of R, then $I = (a)$ (the set of all R-multiples of a) for some $a \in I$.

defn of principal ideal

Theorem

If $R = \mathbf{Z}$ or $R = F[x]$, then R is a PID.

So any ideal of R is the set of all R-multiples of some fixed element of R.

Minimal polynomials

So I is set of all polynomial multiples of d(x).

Definition

Let F be a field, and let I be an ideal of $F[x]$. To say that $d(x)$ is the **minimal polynomial** of I means that $I = (d(x))$. (Exists b/c $F[x]$ PID; turns out to be unique up to associates.)

How compute minimal polynomial? Depends, but in one particular case:

So I is set of all polynomial lin combs of a, b: {r(x)a(x)+s(x)b(x)}

Theorem

Let F be a field, and consider the ideal $I = (a(x), b(x))$ of $F[x]$, where $a(x)$ and $b(x)$ are nonzero polynomials in $F[x]$. Then the minimal polynomial of I is $\gcd(a(x), b(x))$. computed by? yup Euclid Alg

Proof. Let $d(x) = \gcd(a(x), b(x))$. WTS $(d(x)) = (a(x), b(x))$.

First: WTS $(a(x), b(x)) \subseteq (d(x))$.

A: f(x) in (a(x),b(x)), the set of all F[x]-linear combs of a(x), b(x)

To prove that two sets A and B are equal, prove A subset of B and B is a subset of A.
To prove that A subset of B, consider an arbitrary element of A and prove that it must be also an element of B.

So $f(x) = r(x)a(x) + s(x)b(x)$ $(r, s \in F[x])$

$d(x) = gcd(a(x), b(x))$, so divides both.

So a(x)=g(x)d(x) and b(x)=h(x)d(x) for some g(x),h(x) in F[x], which means:

f(x) = r(x)g(x)d(x) + s(x)h(x)d(x) = ~~(r(x)g(x)+s(x)h(x))~~ d(x).

So $f(x) = p(x)d(x)$ for some $p \in F[x]$

C: f(x) in (d(x)), the set of all F[x]-multiples of d(x).

Converse: WTS $(d(x)) \subseteq (a(x), b(x))$.

just rewriting, not inverse

A: f(x) in (d(x)), the set of all F[x]-multiples of d(x)

So f(x) = q(x)d(x) for some q(x) in F[x].

From Euclidean rewriting, we know that d(x) = g(x)a(x) + h(x)b(x) for some g(x),h(x) in F[x]. (Bezout/Euclidean Rewriting for polynomials.)

So f(x) = q(x) (g(x)a(x) + h(x)b(x)) = (q(x)g(x)) a(x) + (q(x)h(x)) b(x).

So f(x) = r(x)a(x) + s(x)b(x) for some r(x), s(x) in F[x].

C: f(x) in (a(x),b(x)), the set of all F[x]-linear combs of a(x), b(x)

If the above seems mysterious, go do the problem from 7.1 where you prove that for a ring R and a,b in R, the set (a,b) = {ra+sb | r,s in R} (set of R-linear combs of a,b) is an ideal of R.

Factorization

For the theory-inclined, proving unique factorization in $\mathbf{Z}$ or $F[x]$ now follows from:

Theorem

If R is a PID, then unique factorization holds in R.

Proof is outside our scope, but that's the key point if you're interested.

7.5: Homomorphisms

And now for something completely different.....

Pretty abstract! But turns out to be surprisingly important for building better codes (codes with larger minimum distances).

Definition

"phi" φ ϕ

Let R and R' be rings. To say that a function $\varphi : R \to R'$ is a **homomorphism** means that for all $r, s \in R$,

$$\varphi(r+s) = \varphi(r) + \varphi(s), \qquad \varphi(rs) = \varphi(r)\varphi(s).$$

In other words, a homomorphism is a function between rings that preserves addition and multiplication.

Example: Quotient rings

Let R be a ring, and let I be an ideal of R.
Define $\varphi : R \to R/I$ by (R/I is the set of all (additive) cosets of I in R)

$$\varphi(r) = r + I$$

for all $r \in R$.
The two conditions of the definition of homomorphism become

$$(r+s)+I = (r+I)+(s+I) \qquad (rs)+I = (r+I)(s+I),$$

(these are exactly the defn of + and * in R/I)
which hold by defn of R/I. (In fact, defn really chosen to make φ a homomorphism.)

φ is **canonical homomorphism** from R to R/I.

Ex of example: phi: Z -> Z/(7), so phi squishes together 0,7,14,21,28,....

Example: Substitution

$F = \mathbb{Q}, \mathbb{R}, \mathbb{C}, F_p$

F a field, $\alpha \in F$. Define $\varphi : F[x] \to F$ by

(inputs polynomials, outputs elements of F)

$$\varphi(f(x)) = f(\alpha)$$

for all $f(x) \in F[x]$. Turns out φ is a homomorphism, i.e.: e.g.:

$\varphi(f(x)+g(x)) = \varphi((f+g)(x))$ result of adding polynomials

$= (f+g)(\alpha)$ ← then plug in alpha

First property of homomorphisms says these are equal

vs.

$\varphi(f(x)) + \varphi(g(x)) = f(\alpha) + g(\alpha)$

substitute alpha first, then add results

(and similarly for multiplication)

I.e., doesn't matter if you substitute before or after adding/multiplying.

Notation makes this look natural because f, g written as functions.

First properties of homomorphisms

Theorem

Let R and R' be rings, with additive identity elements 0 and $0'$, and let $\varphi : R \to R'$ be a homomorphism. Then:

(a) ▶ $\varphi(0) = 0'$. Homomorphisms preserve zero element

(b) ▶ *For all $r \in R$, $\varphi(-r) = -\varphi(r)$.* Homomorphism send negatives to negatives.

Proof of (b).

Let $r \in R$, φ homom. Then

$\varphi(r) + \varphi(-r) = \varphi(r + (-r)) = \varphi(0) = 0'$

Subtr $\varphi(r)$: $\varphi(-r) = 0' - \varphi(r) = -\varphi(r)$.

C. $\varphi(-r) = -\varphi(r)$

Theorem

Let R, R', and R'' be rings, and let $\varphi : R \to R'$ and ρ ("rho") $: R' \to R''$ be homomorphisms. Then $(\rho \circ \varphi) : R \to R''$ is a homomorphism.

Proof: PS09.

Isomorphisms

Definition

An **isomorphism** is a bijective (one-to-one and onto) homomorphism. To say that rings R and R' are **isomorphic** means that there exists some isomorphism $\varphi : R \to R'$.

If an isomorphism $\varphi : R \to R'$ exists, then because φ is a bijective correspondence and preserves the ring operations, R and R' are fundamentally the same algebraic object, just with different names for their elements. Conversely, if R and R' have different algebraic properties, they can't be isomorphic.

E.g., if you take Z/(3)={0,1,2} and rename elements {Moe,Larry,Curly} but preserve all of algebraic operations (e.g., Larry+Curly=Moe), then you haven't really made a new ring; you're just using different names for the old ring. So we say {Moe,Larry,Curly} is isomorphic to Z/(3).

Properties preserved by isomorphisms

If rings R and R' are isomorphic, then:

- R and R' have the same number of elements.
- R and R' have the same number of units.
- R is an integral domain if and only if R' is an integral domain.
- R is a field if and only if R' is a field.
- R is a PID if and only if R' is a PID.

In fact, if I'm not being fussy, I just say that R and R' are "the same ring".

Example

$F_2(\alpha)$ $F_2(\beta)$

Let $R_1 = \mathbf{F}_2[x]/(x^2+1)$, $R_2 = \mathbf{F}_2[x]/(x^2+x+1)$, $R_3 = \mathbf{Z}/(4)$. Are these rings isomorphic? Look for abstractly stated properties that distinguish them to prove not.

Since $R_1 = \{0, 1, \alpha, \alpha+1\}$

$R_2 = \{0, 1, \beta, \beta+1\}$

$R_3 = \{0, 1, 2, 3\}$

All three rings have same number of elements, so could be isomorphic so far....

But it turns out that these three rings are pairwise *not* isomorphic, ie.., all three of them are different. We show this by finding abstract properties that distinguish the three rings. Example:

In R_1, $\alpha^2+1 = 0, \text{so}$

$(\alpha+1)^2 = \alpha^2+1 \quad \alpha+1 = \alpha^2+1 = 0 \pmod{\alpha^2+1}$ (still mod 2)

In R_3, $2 \cdot 2 = 0$.

R1 and R3 have zero divisors!

But x^2+x+1 is irreducible over F_2, so R_2=F_2[x]/(x^2+x+1) is field.

So R_2 is not isom to R_1 or R_3. Can also show that R_1, R_3 not isom.

Automorphisms

Definition

An **automorphism** is an isomorphism $\varphi : R \to R$ from a ring to itself.

Example: For $R = \mathbf{C}$ (complex numbers), define $\varphi : \mathbf{C} \to \mathbf{C}$ by

$$\varphi(a + bi) = a - bi \tag{1}$$

for $a, b \in \mathbf{R}$. Then φ is a homomorphism (check) and $\varphi^{-1} = \varphi$, so φ is an isomorphism, and therefore, an automorphism of $\mathbf{C}$.

Induced automorphism on polynomials

Example: R a ring, $\varphi : R \to R$ be an automorphism of R. Define a map $\Phi : R[x] \to R[x]$ by saying for $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$,

$$(\Phi(f))(x) = \varphi(a_n)x^n + \cdots + \varphi(a_1)x + \varphi(a_0). \tag{2}$$

I.e., we get $(\Phi(f))(x)$ by applying φ to the *coefficients* of $f(x)$. Then Φ is an automorphism of $R[x]$, called the **automorphism of** $R[x]$ **induced by** φ.

Induced automorphism and roots of a polynomial

Theorem

Let R be a ring, let $\varphi : R \to R$ be an automorphism of R, and let $\Phi : R[x] \to R[x]$ be the corresponding induced automorphism. Then for $f(x) \in R[x]$ and $\alpha \in R$, if $f(\alpha) = 0$, then $(\Phi(f))(\varphi(\alpha)) = 0$.

I.e., an induced automorphism sends roots to roots.

Example: Suppose $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is a polynomial with **real** coefficients, and suppose α is a complex root of $f(x)$.

7.6: Finite fields, first defns

Today: Try to introduce enough definitions to state the main facts about finite fields.

Definition

The **order** of a field F is defined to be the number of elements in F; a **finite field** is therefore the same as a field of finite order.

Definition

Let R be a ring. Since R has a multiplicative identity 1, for a positive integer n, we can abbreviate

$$n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ times}}. \tag{3}$$

Then define $\mathrm{char}(R)$, the **characteristic** of R, by:

- If $n \cdot 1 = 0$ for some positive integer n, then $\mathrm{char}(R)$ is smallest positive n such that $n \cdot 1 = 0$.
- If $n \cdot 1 \neq 0$ for all positive integers n, then $\mathrm{char}(R) = 0$.

Finite fields: Multiplicative group

Definition

Let F be a field. We use $F^\times$ to denote the set of all nonzero elements of F, all of which are units (since F is a field). We therefore call $F^\times$ the **multiplicative group** of F.

Note the new (and not yet defined) term **group** here.

Definition

Let $F^\times$ be the multiplicative group of the field F, and suppose $\alpha \in F^\times$. To say that $F^\times$ is **cyclic** means that there exists some $\alpha \in F^\times$ such that every element of $F^\times$ is some power of α, in which case we say that α is a **primitive** element of F.

(We saw primitive elements back when we first introduced $\mathbf{Z}/(m)$.)

Five Facts For Finite Fields

1. The characteristic of a finite field must be a prime p, and its order must be $q = p^e$ for some $e \geq 1$.
2. Every finite field has a primitive element.
3. If F is a field of order q, then every $\alpha \in F$ is a root of $x^q - x$, or in other words, $\alpha^q = \alpha$ for every $\alpha \in F$. Consequently, $x^q - x$ factors as the product of all $(x - \beta)$, where β runs over all elements of F (including $0 \in F$).
4. Every finite field of characteristic p is isomorphic to $\mathbf{F}_p[x]/(m(x))$ for some irreducible polynomial $m(x)$.
5. For any prime p and $q = p^e$ $(e \geq 1)$, there exists a field $\mathbf{F}_q$ of order q that is unique up to isomorphism.